

# PRIVACY BELEVING

## OP HET INTERNET IN NEDERLAND

innovation for life

RAPPORT

FEBRUARI 2015

# COLOFON

Arnold Roosendaal, Ottilie Nieuwenhuis, Merel Ooms,
Anita Bouman-Eijs en Noor Huijboom

Met dank aan Tijs van den Broek

Februari 2015

TNO 2015 R10276

**TNO.NL**

# INHOUD

HOE VAAK DENKT U NA OVER

# DE GEVOLGEN VAN INTERNETGEBRUIK VOOR UW PERSOONSGEGEVENS?



# SAMENVATTING

DIT RAPPORT BEVAT DE BEVINDINGEN VAN EEN SURVEY ONDER EEN REPRESENTATIEVE STEEKPROEF VAN DE NEDERLANDSE BEVOLKING OVER DE BELEVING VAN PRIVACY OP HET INTERNET. DEZE BELEVING HEBBEN WE ONDERZOCHT AAN DE HAND VAN EEN ZEVENTAL FACTOREN: PERSOONSKENMERKEN, ERVARINGEN, FEITELIJK GEDRAG, CONTEXT, TECHNOLOGIE, INVLOED & CONTROLE EN AWARENESS. EEN PRIVACY-BELEVING BLIJKT VAN MEERDERE FACTOREN EN PARTIJEN AFHANKELIJK TE ZIJN.

Uit het onderzoek blijkt dat de Nederlandse bevolking veel belang hecht aan privacy en de bescherming van persoonsgegevens: 82,5% van de respondenten vindt dit belangrijk. Er worden ook concrete acties ondernomen om persoonsgegevens te beschermen, zoals het installeren van beschermende software (88,5%) of het aanpassen van profielinstellingen (68,4%). Tevens zijn veel mensen terughoudend in het delen van gegevens als het doel of de noodzaak daarvan niet geheel duidelijk zijn (respectievelijk 38,6% en 29,5%). Opvallend is dat mensen die veel maatregelen hebben getroffen om gegevens te beschermen, zoals beschermende software installeren, veel minder vaak navraag doen naar het verwerken van hun gegevens. De mogelijkheid tot controle en het gevoel van controle leiden dus tot meer vertrouwen in een zorgvuldige verwerking.

Hoewel er actief wordt geprobeerd controle te houden over persoonsgegevens, zijn er veel situaties waar dat lastig of onmogelijk is. Bijvoorbeeld doordat consumenten niet kunnen zien wie hun gegevens verzamelen. Zo zijn er commerciële partijen die met tracking tools persoonsgegevens verzamelen zonder dat consumenten dit weten. De Nederlandse bevolking heeft dan ook een negatieve houding ten opzichte van dergelijke technologieën. Daarnaast heeft men weinig vertrouwen in een goede omgang met persoonsgegevens door commerciële partijen, zoals webwinkels, sociale netwerksites, en ook goede doelenorganisaties (respectievelijk 58,4%, 74,8% en 50,5% heeft weinig tot zeer weinig vertrouwen). Overheidsorganisaties zoals de politie en de belastingdienst worden daarin meer vertrouwd (respectievelijk 45,5% en 43,2% heeft veel tot zeer veel vertrouwen).

Ondanks het gebrek aan vertrouwen, nemen mensen wel deel aan sociale netwerksites, onder andere omdat de omgeving daar om vraagt. Hier is dus sprake van peer pressure. Ook is er een groep internetgebruikers die weinig moeite heeft met het delen van persoonsgegevens in ruil voor een gratis dienst (17,4% voelt zich hierbij gemakkelijk en 44,9% neutraal). De privacy paradox bestaat: mensen zeggen privacy belangrijk te vinden, maar handelen er niet naar. Wel is gebleken dat in veel gevallen een afgewogen keuze wordt gemaakt over het delen van persoonsgegevens: de context waarin gegevens worden gedeeld en wat daar tegenover staat is van belang bij de keuze. Als alleen een commerciële partij er geld mee verdient, is er meer weerstand en worden er, indien mogelijk, geen gegevens gedeeld. In andere gevallen blijkt er echter geen keuze te zijn om het delen van gegevens te weigeren, omdat anders de dienst bijvoorbeeld niet toegankelijk is.

HOEVEEL UUR PER

# DAG MAAKT U GEMIDDELD GEBRUIK VAN HET INTERNET?



# 1 INLEIDING

PRIVACY IS DAGELIJKS IN HET NIEUWS. VAAK IS DAT IN NEGATIEVE ZIN, BIJVOORBEELD OMDAT ER GEGEVENS VAN PERSONEN ZIJN GELEKT UIT EEN SLECHT BEVEILIGDE DATABANK, OMDAT VEILIGHEIDSDIENSTEN OP GROTE SCHAAL BURGERS AFLUISTEREN, OF OMDAT BANKEN AANGEVEN DAT ZE TRANSACTIEGEGEVENS VAN KLANTEN WILLEN GAAN GEBRUIKEN OM PERSOONLIJKE AANBIEDINGEN TE DOEN. DEZE ZORG OM PRIVACY BIEDT OOK KANSEN VOOR INNOVATIE.

TNO heeft een aantal van deze innovaties uitgewerkt in het Actieplan Privacy, vergezeld van beleidsaanbevelingen om privacy innovatie te stimuleren. De grote maatschappelijke aandacht voor privacy betekent in ieder geval dat consumenten het een belangrijk onderwerp vinden en over het algemeen meer privacybewust zijn dan enkele jaren geleden. Nieuwe diensten of technologieën worden kritischer bekeken dan voorheen. Ook is duidelijk dat het begrip privacy niet eenduidig is en dat niet iedereen er dezelfde betekenis aan toekent.

**Privacy en vertrouwen**

Negatieve voorbeelden hebben tot gevolg dat burgers niet altijd vertrouwen hebben in online diensten en dat sommige online diensten daarom ook niet gebruikt worden. Naast privacy die in het geding is worden diensten soms niet gebruikt vanwege gebrekkige beveiliging, slechte beschikbaarheid of onacceptabele voorwaarden. Het niet waarborgen van privacy wordt echter wel als belangrijkste reden naar voren gebracht.

De toegenomen aandacht voor privacy kan zijn weerslag hebben op de economie. Het al dan niet slagen van nieuwe diensten of producten kan afhangen van de publieke perceptie en acceptatie. Voldoen aan de wettelijke vereisten is niet altijd voldoende om een dienst te laten slagen. Wanneer voor een dienst persoonsgegevens van gebruikers worden verwerkt, dan is de wijze van communiceren en uitleggen wat er gebeurt met de gegevens essentieel.

Los van het tegengaan of voorkomen van economische gevolgen die mogelijk kunnen ontstaan door slechte bescherming van privacy door bedrijven, heeft de overheid ook als taak om de privacy van haar burgers te waarborgen. Privacy is een fundamenteel recht dat bescherming verdient en alleen onder bepaalde voorwaarden mag worden ingeperkt. De discussie over privacy wordt echter bemoeilijkt doordat verschillende contexten (overheid, veiligheid, commercieel) waarin privacy een rol speelt door elkaar lopen. Het gevolg is dat de beleving van privacy bij het gebruik van commerciele diensten, beïnvloed kan worden door berichtgeving over overheidssurveillance. Ook treden er

verschillen op tussen privacy in de fysieke ruimte en privacy op het internet. Op het internet kan de gebruiker bijna altijd ongemerkt gevolgd worden. Offline zijn de technieken, zoals camera's en scanners, vaak zichtbaar.

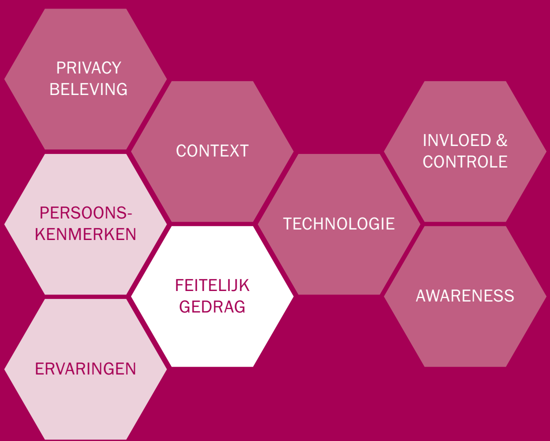
Als antwoord op discussie in de Tweede Kamer, heeft het Ministerie van Economische Zaken TNO verzocht om een onderzoek uit te voeren naar de privacybeleving van burgers in Nederland, in het bijzonder op het internet en online dienstverlening. Met dit onderzoek wil het Ministerie inzicht krijgen in de maatschappelijke visie op privacy en de mate waarin volgens consumenten privacy geborgd is. Door middel van een survey heeft TNO de beleving van privacy en de borging hiervan onder de Nederlandse bevolking gepeild. De resultaten van de survey zijn in dit rapport weergegeven.

HEEFT UW WEL EENS

# TE MAKEN GEHAD MET VERLIES OF DIEFSTAL VAN UW PERSOONSGEGEVENS?



# LEEST U DE ALGEMENE **VOORWAARDEN VOOR U GEBRUIK MAAKT VAN EEN DIENST?**



# 2 METHODE

OM INZICHT TE GEVEN IN DE PRIVACYBELEVING VAN NEDERLANDSE SAMENLEVING, IS EEN SURVEY UITGEVOERD ONDER 1000+ NEDERLANDSE CONSUMENTEN, REPRESENTATIEF NAAR LEEFTIJD, GESLACHT EN REGIO. IN DIT HOOFDSTUK LICHTEN WE TOE HOE DE SURVEY EN DATASET TOT STAND ZIJN GEKOMEN.

Bij het samenstellen van de survey is een vragenlijst gebruikt die werd ingebracht door het Ministerie van Economische Zaken en het College Bescherming Persoonsgegevens.
Deze vragenlijst is als vertrekpunt gebruikt. Aanvullend daarop is aan enkele maatschappelijke organisaties die actief zijn op het gebied van privacy in Nederland, namelijk Bits of Freedom en de Consumentenbond, gevraagd welke onderwerpen zij van belang achten. De inbreng van deze organisaties is waar mogelijk en relevant meegenomen in de uiteindelijke survey. Vervolgens is deze survey nog aangevuld met relevante vragen uit eerdere surveys die nationaal en internationaal hebben plaatsgevonden, zoals de PRISMS survey die TNO in Europees verband heeft uitgevoerd.

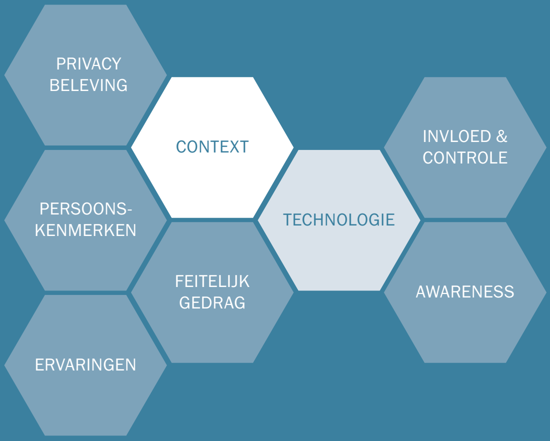
Na voltooiing van de vragenlijst heeft een pretest plaatsgevonden en is de vragenlijst op 7 januari 2015 door Survey Sampling International (SSI) uitgezet onder de respondenten. Op 12 januari 2015 is een opgeschoonde dataset aan TNO overhandigd.

Een uitgebreide omschrijving van de dataset volgt in hoofdstuk 4, waar ook de resultaten van het onderzoek zullen worden besproken. Bij de complete dataset moet nog een kanttekening worden geplaatst, omdat tijdens het afnemen van de vragenlijst aanslagen plaatsvonden in Parijs op een Joodse supermarkt en satirisch dagblad Charlie Hebdo.

Om vast te kunnen stellen of deze aanslagen van invloed zijn geweest op de privacybeleving van de respondenten en daarmee een vertekend beeld hebben gegeven in de dataset, hebben we een ANCOVA-analyse uitgevoerd ($p < 0.05$). Daarbij is er gekeken of de data die zijn verzameld na het bekend worden van de aanslagen substantieel afwijken van de data vóór het bekend worden van de aanslagen.

Uit de analyse blijkt dat enkele items waarin gekeken wordt naar het belang dat de respondenten hechten aan het controleren en privé houden van hun persoonsgegevens significant blijken af te wijken ná de aanslagen in Parijs. Het gaat dan specifiek om het kunnen voeren van telefoongesprekken, het kunnen deelnemen aan een demonstratie en het kunnen ontmoeten van mensen zonder dat overheden meekijken. Het lijkt er op dat de respondenten – misschien tijdelijk – onder invloed van de aanslagen meer bereid zijn geweest om hun privacy op te geven als daarmee hun veiligheid wordt gewaarborgd. Op de overige vragen zijn geen significante verschillen gevonden, wat leidt tot de conclusie dat de invloed van de aanslagen op de dataset zeer beperkt is.
De afwijkende items zullen in ieder geval met enig voorbehoud worden behandeld.

HOEVEEL VERTROUWEN
# HEEFT U IN COMMERCIËLE ONLINE DIENSTENAANBIEDERS?



# 3 THEORETISCHE ACHTERGROND

IN DIT HOOFDSTUK ZULLEN WE UITLEG GEVEN AAN HET BEGRIP PRIVACYBELEVING. WE ZULLEN KIJKEN NAAR SOORTGELIJK ONDERZOEK IN HET BUITENLAND EN UITEENZETTEN WELKE FACTOREN VAN INVLOED ZIJN OP DE PRIVACYBELEVING OP HET INTERNET IN NEDERLAND.

Er zal geen algemeen beeld bestaan van het concept privacy, dat van toepassing is op alle burgers. Dit maakt het nodig om te achterhalen waarom iemand een bepaalde beleving heeft van zijn of haar privacy. Is bijvoorbeeld de leeftijd of het geslacht van belang bij deze beleving? Heeft het te maken met eerdere ervaringen? Of gaat het vooral om de controle die men heeft over het gebruik? En zijn er verschillen waarneembaar in de privacybeleving van burgers bij verschillende technologieën of verschillende situaties waarin gegevens verwerkt worden? Deze vragen vormden de achtergrond voor het door TNO ontwikkelde survey.

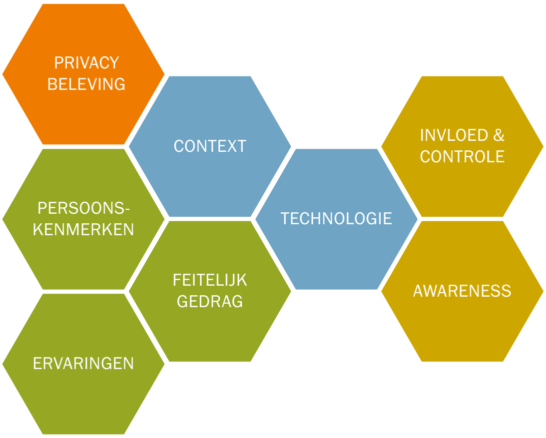
**Privacybeleving in eerder onderzoek**

Uit soortgelijk onderzoek in het buitenland blijkt dat online diensten vaak als een risico voor privacy worden gezien. In Australië noemt bijvoorbeeld 48% van de mensen dit spontaan als belangrijkste risico. Onder jongeren in Australië is dit zelfs 60%. In Canada is twee derde van de bevolking bezorgd over zijn of haar privacy en een kwart zelfs zeer bezorgd. Een Amerikaanse survey wijst uit dat 50% van de Amerikanen zich zorgen maakt over de hoeveelheid informatie die online over hen beschikbaar is, terwijl dit in 2009 nog ‘slechts’ 33% was. Ook een wereldwijde studie van UNESCO geeft aan dat het internet een aantal nieuwe uitdagingen met zich meebrengt voor de bescherming van privacy. Dat is met name te wijten aan een vijftal kenmerken van het internet dat UNESCO heeft onderscheiden: (1) het faciliteert het verzamelen van nieuwe typen gegevens; (2) het faciliteert het verzamelen en lokaliseren van persoonsgegevens; (3) het biedt nieuwe mogelijkheden voor overheden en private actoren om gegevens te analyseren; (4) het biedt nieuwe kansen voor het commerciële gebruik van persoonsgegevens en (5) het creëert nieuwe uitdagingen voor regelgeving vanwege het transnationale karakter. De beleving van privacy kan door deze karakteristieken van het internet beïnvloedt worden, bijvoorbeeld omdat er – doordat er zo gemakkelijk gegevens verzameld en geanalyseerd kunnen worden – een gevoel van gebrek aan controle over gegevens of gebrek aan handhaving bij inbreuken op wet- en regelgeving kan ontstaan.

Een onderzoek in opdracht van E-Commerce Platform Nederland (ECP) wijst uit dat ook Nederlanders hun privacy belangrijk vinden en dat hun informatie vertrouwelijk blijft (86%). De personen die gemakkelijker informatie delen hebben ook meer vertrouwen in een zorgvuldige omgang met die gegevens. Ook lijkt het al dan niet delen van gegevens meer af te hangen van de persoon en zijn opinie, dan van de specifieke situatie.

Om de privacybeleving van de Nederlandse samenleving in kaart te brengen, is een aantal factoren te onderscheiden. Dit kunnen persoonlijke factoren zijn (bijvoorbeeld persoonskenmerken, ervaringen en feitelijk gedrag), maar ook contextuele (zoals de context of het type technologie dat is toegepast) of randvoorwaarden scheppende factoren (bijvoorbeeld de mate waarin men invloed heeft op het gebruik van gegevens en de kennis die men heeft over de partijen die hier mee bezig zijn).

Om het begrip privacybeleving te meten, hebben we er in dit onderzoek voor gekozen om voort te bouwen op een clustering van de eerder onderscheiden factoren die van invloed zijn op de privacybeleving. Het gaat daarbij om: (1) *persoonskenmerken* zoals geslacht, leeftijd, opleidingsniveau en hoeveelheid uren per dag dat internet wordt gebruikt; (2) *ervaringen* met verlies of diefstal van gegevens, identiteitsfraude en het vertrouwen in het optreden van de overheid; (3) *feitelijk gedag*, zoals het gebruik van bepaalde diensten, de bereidheid om gegevens af te staan en het lezen van algemene voorwaarden; (4) de *context* waarin bepaalde organisaties en actoren om gegevens vragen en vertrouwd worden; (5) het type *technologie* dat gebruikt wordt om persoonsgegevens te verzamelen en verder te verwerken; (6) de behoefte aan en het uitoefenen van *invloed & controle* over de gegevens en het omgaan met druk uit de omgeving en tot slot (7) de kennis of *awareness* over het maatschappelijk speelveld en debat.




De verwachting is dat deze factoren veelal in samenhang voorkomen, omdat ze sterk aan elkaar gerelateerd zijn en elkaar beïnvloeden. Zo kan bijvoorbeeld het *feitelijk gedrag* dat een gebruiker vertoont sterk afhangen van de *controle* die hij heeft over het gebruik van zijn gegevens door anderen. In het hoofdstuk over de resultaten van deze survey zal ernaar gestreefd worden om eventuele correlaties tussen factoren weer te geven. In de volgende paragrafen zullen relevante factoren van de zeven gebieden beschreven worden en waar mogelijk verwachtingen worden uitgesproken over de uitkomsten van het onderzoek.

**Algemene houding ten aanzien van privacy**
Allereerst zal de algemene houding ten aanzien van privacy onder de respondenten in kaart worden gebracht. De algemene houding zegt iets over de mate waarin iemand privacy en de bescherming van persoonsgegevens van belang acht en zichzelf privacybewust vindt. Deze houding vormt het vertrekpunt voor nadere analyse en vergelijking van de uitkomsten. Zo zal iemand die zichzelf meer

privacybewust vindt, in het verlengde daarvan, een meer kritische houding aannemen ten aanzien van het verstrekken of gebruik van persoonsgegevens. Deze houding is vervolgens weer van invloed op de beleving die iemand heeft: iemand die bescherming van persoonsgegevens belangrijk vindt, zal het doorverkopen van gegevens aan derden anders ervaren dan iemand die dat een normaal verschijnsel vindt in de huidige samenleving en dus minder kritisch zal zijn.

## 3.1 PERSOONSKENMERKEN

Voor de survey is gekozen voor een representatieve steekproef van de inwoners van Nederland, waardoor eventuele verschillen op basis van demografische kenmerken zoals leeftijd, geslacht en opleiding naar voren kunnen komen. Zo valt te verwachten dat jongeren en jongvolwassenen die meer tijd doorbrengen op het internet en gewend zijn geraakt aan het delen van welhaast ongelimiteerde berichten, foto's en video's op sociale media – de zogenaamde Facebookgeneratie – ook minder moeite hebben met het delen van gegevens dan oudere generaties. Er verschijnt overigens al onderzoek dat het overmatige delen van de Facebookgeneratie enigszins afzwakt[1]: het delen van informatie online is niet meer dan een equivalent van wat altijd al offline gebeurde. Door de mogelijkheden van het internet (zoals ook omschreven door UNESCO) is de informatie echter breder te delen en zijn de gevolgen verderstrekkend dan in het verleden het geval was. Naarmate jongeren ouder worden groeit echter ook hun besef van privacy en worden ze voorzichtiger.

Daarnaast zal worden onderzocht of de hoeveelheid uren per dag dat iemand gebruik maakt van internet voor privédoeleinden samenhangt met de houding die iemand heeft tegenover het (commercieel) gebruik van persoonsgegevens. Bij de meeste online activiteiten vindt namelijk uitwisseling van persoonsgegevens plaats, of het nu gaat om het doen van online aankopen, het surfen op websites of het plaatsen van berichten op sociale media. De verwachting is dat mensen die meer gewend zijn gegevens te delen, ook meer gebruik maken van diensten die persoonsgegevens verwerken – zoals webwinkels en sociale media.

## 3.2 ERVARINGEN

Eerdere ervaringen die mensen hebben gehad met verlies of misbruik van persoonsgegevens, vormen belangrijke voorspellers voor de privacybeleving. Zo zal naar verwachting iemand die te maken heeft gehad met diefstal en misbruik van creditcardgegevens, hier in het vervolg waarschijnlijk voorzichtiger mee omgaan – om herhaling te voorkomen. En dus ook kritischer zijn als het gaat om bescherming van zijn of haar gegevens.

Bij het in kaart brengen van persoonlijke ervaringen wordt de mogelijkheid voor longitudinaal onderzoek geopend. In het algemeen is gevraagd of iemand weleens te maken heeft gehad met een incident of andere negatieve ervaring. Indien dit het geval is, is ook de vraag gesteld of dit in het afgelopen jaar is gebeurd. Bij eventuele herhalingen van de survey kan op die wijze een vergelijking tussen verschillende jaren in kaart worden gebracht, waarmee duidelijk wordt of er in het algemeen eventueel een toename of afname is van het aantal incidenten of andere negatieve ervaringen.

Het is echter de vraag of mensen zich altijd bewust zijn van het feit dat zij slachtoffer zijn geweest van verlies, diefstal of misbruik van persoonsgegevens. Zo kunnen er gegevens van iemand zijn gestolen bij een andere organisatie, zonder dat deze organisatie dit door heeft gehad. Tevens is het

1 Steijn, W.M.P. (2014). Developing a Sense of Privacy. Proefschrift Tilburg University, p. 204.

mogelijk dat de organisatie wel van het verlies op de hoogte is, maar dit niet heeft gecommuniceerd richting de consument.

Ook zullen we in ogenschouw nemen hoe men de bescherming door het overheidsbeleid en het kader van wet- en regelgeving ervaart. De mate waarin mensen zich beschermd voelen en gesterkt voelen door wet- en regelgeving, zal de algemene houding beïnvloeden. Immers, iemand die er op vertrouwt dat de overheid optreedt bij onrechtmatig handelen, zal meer vertrouwen hebben in goede afloop en anticiperend hierop mogelijk meer risico nemen.

## 3.3 FEITELIJK GEDRAG

Naast de tijd die mensen doorbrengen op internet, zullen we hen ook vragen welke type diensten ze precies gebruiken (e-mail, zoekmachines, mobiele applicaties, et cetera).

Uit recent tijdsbestedingsonderzoek van het Sociaal Cultureel Planbureau bleek al dat 23% van de Nederlanders dagelijks tijd door brengt op sociale media tot wel anderhalf uur per dag. Het percentage flitsbezoekers van sociale media, die per keer minder dan 5 minuten op sociale media doorbrengen, ligt zelfs op 50% van de Nederlandse bevolking[2].

Het gebruik van typen diensten willen we vervolgens afzetten tegen de algemene houding ten aanzien van privacy: maken mensen die de bescherming van hun persoonsgegevens belangrijk vinden ook minder gebruik van diensten die om dergelijke gegevens vragen? En als ze gebruik maken van het internet, in welke mate zijn zij dan bereid om persoonsgegevens te verstrekken? De beleving van privacy lijkt een belangrijke voorspeller voor het gedrag dat wordt vertoond om privacy te beschermen. Immers, als je je zorgen maakt over je privacy, dan ga je ook zorgvuldiger om met het delen van je gegevens.

Volgens de privacy paradox is echter het tegengestelde vaak het geval: mensen zeggen privacy belangrijk te vinden, maar handelen er vervolgens niet naar als ze allerlei persoonsgegevens achterlaten, bijvoorbeeld op hun profiel op Facebook. Gedachten en gedrag komen dan niet overeen. Het hoge percentage (dagelijkse) gebruikers van sociale media lijkt hier ook op te wijzen: sociale media zijn bij uitstek platformen die voortbestaan op basis van de informatie die de gebruikers met elkaar delen. Ondanks de risico's voor de bescherming van persoonsgegevens die daarmee gepaard gaan, maken veel mensen paradoxaal genoeg toch intensief gebruik van deze diensten.

Ook in literatuur uit de hoek van behavioural economics komt een soortgelijk tegenstrijdig gedrag naar voren: hoewel privacy belangrijk wordt gevonden, hebben consumenten een erg beperkte bereidheid om te betalen voor de bescherming ervan.[3] Het snelle financieel voordeel wordt over het algemeen als aantrekkelijker beschouwd. Daardoor wordt vaak ook de waarde van persoonsgegevens erg laag ingeschat.[4]

Een andere vorm van gedrag waarbij de privacy paradox zichtbaar wordt, is het lezen van de algemene voorwaarden. Algemene voorwaarden kunnen informatie verschaffen over het gebruik van bepaalde persoonsgegevens. Aanbieders van internetdiensten zijn daartoe ook verplicht: ze moeten er zorg voor dragen dat gebruikers voldoende geïnformeerd zijn over de verwerking van

2 SCP (2015) Media: Tijd in beeld. Dagelijkse tijdsbesteding aan media en communicatie.
3 Acquisti, A. (2009). Nudging privacy: The behavioural economics of personal information. IEEE Security and Privacy, 72-75.
4 Spiekermann, S. (2012). Privacy property and personal information markets. Acatech - Deutsche Academie der Wissenschaften. Berlin.

hun persoonsgegevens en om welke gegevens het precies gaat en voor welk doel ze worden verwerkt. Veel internetdiensten beschouwen de algemene voorwaarden als voldoende informatief om van geïnformeerde toestemming te kunnen spreken voor het verwerken van iemands persoonsgegevens. Deze voorwaarden worden echter door de helft van de mensen niet gelezen. In Australië leest bijvoorbeeld 51% van de internetgebruikers de algemene voorwaarden niet, omdat deze te lang (52%), te complex (20%) of te saai zijn (9%). Van de mensen in Australië die de algemene voorwaarden wel leest, geeft 37% aan er ook de benodigde informatie uit halen om te bepalen of ze de dienst willen gebruiken of niet.[5] In Canada leest ook de helft van de gebruikers geen algemene voorwaarden, 62% geeft aan dat de algemene voorwaarden doorgaans vaag en onduidelijk zijn. Met als gevolg dat veel mensen instemmen met voorwaarden waar ze eigenlijk niet achter staan. Slechts 21% van de Canadezen leest de voorwaarden vaak of altijd.[6] Van die 21% heeft 68% weleens een site of dienst niet gebruikt, omdat ze zich niet konden vinden in de voorwaarden van de dienst.[7] Hoewel men zich onvoldoende geïnformeerd voelt, kiest men er toch voor om de algemene voorwaarden te accepteren en gebruik te maken van een dienst waarbij persoonsgegevens verzameld en gebruikt (kunnen) worden. Ook hier sluiten gedachten en gedrag niet op elkaar aan. De verwachting is dat dit in Nederland hetzelfde zal zijn.

### 3.4 CONTEXT

De mate waarin iemand zijn of haar gegevens beschermt of beschermd wil zien, kan ook afhangen van de context[8] waarin deze gegevens gevraagd worden, bijvoorbeeld een medische omgeving, bij arbeidsrelaties, voor commerciële toepassingen, of bij privé aangelegenheden. Medische gegevens zijn wettelijk gekwalificeerd als gevoelige gegevens en de verwerking daarvan is aan strenge eisen onderworpen. Strenger dan voor veel andere gegevens. De houding van een consument ten aanzien van de verwerking van medische gegevens kan echter verschillen al naar gelang de instelling of persoon die de gegevens verwerkt. En het doel waarvoor deze gegevens verwerkt worden. Van een arts wordt verwacht dat hij in het kader van een medische behandeling gegevens verwerkt. Wanneer een verzekeraar toegang verlangt tot dezelfde gegevens, dan wordt het al gevoeliger omdat daar mogelijk het weigeren van het delen van gegevens door een patiënt ook kan leiden tot het weigeren van een aanvullende verzekering door de verzekeraar. En men zal zijn medische dossier ook niet zomaar aan een werkgever toevertrouwen. Wettelijk gezien heeft een werkgever daar ook geen recht op, maar dient dit vertrouwelijk behandeld te worden door een Arboarts als het relevant kan zijn voor het arbeidsproces.

De context, de betrokken actoren en het type gegevens zijn dus belangrijke factoren die van invloed zijn op de beleving van privacy. Ook het doel waarvoor de gegevens verzameld en verwerkt worden is van belang. De houding ten aanzien van gegevensverwerking voor gezondheidsdoeleinden zal heel anders zijn dan verwerking van gegevens voor veiligheidsdoeleinden. Een geheel andere houding wordt verwacht ten aanzien van de verwerking van persoonsgegevens voor commerciële doeleinden. Uit een survey die is uitgevoerd in het kader van het PRISMS-project[9] is reeds gebleken dat mensen een negatievere houding hebben ten aanzien van de verwerking van gegevens voor commerciële doeleinden dan voor veiligheidsdoeleinden. Commercieel gebruik van gegevens wordt dan ook vrij veel afgewezen.

5 Office of the Australian Information Commissioner (2013). Community Attitudes to Privacy Survey, research report 2013.
6 Phoenix (2013). Survey of Canadians on Privacy-Related Issues, Prepared for the Office of the Privacy Commissioner of Canada, January 2013.
7 Idem.
8 Zie ook: H. Nissenbaum (2009) Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford Law Books.
9 Zie http://prismsproject.eu/. Het PRISMS-project is een Europees onderzoeksproject waarin de trade-off tussen privacy en veiligheid wordt bevraagd.

Om het vertrouwen in de verschillende contexten te meten, zullen we respondenten vragen in welke mate ze bepaalde partijen vertrouwen. We zullen daarbij onderscheid maken naar verschillende typen overheidsinstellingen en commerciële organisaties. Ook zullen we respondenten vragen in hoeverre zij bereid zijn hun gegevens te delen in ruil voor gratis diensten. Het doel (verzamelen van gegevens) wordt dan vervangen door een gunst (gratis gebruik maken van een dienst): zijn respondenten dan meer bereid om hun gegevens te verstrekken? En hoe verhoud zich dit tot hun algemene houding ten aanzien van privacy? Zijn respondenten die sowieso meer bereid zijn gegevens te delen ook meer bereid hun gegevens te delen in ruil voor gratis diensten?

## 3.5 TECHNOLOGIEËN

Er worden in het dagelijks leven verschillende technieken gebruikt om gegevens te registreren. Zo zijn er in het straatbeeld camera's en op vliegvelden bodyscanners zichtbaar. Daarnaast worden er door zowel overheden als commerciële partijen online technologieën ingezet om het internetverkeer in de gaten te houden. De ene techniek is dus meer zichtbaar dan de andere. Ook verschilt het doel waarvoor de technologie gebruikt kan worden: de camera's en bodyscanners worden veelal ingezet voor veiligheidsdoeleinden, terwijl het registreren van internetverkeer vaak gebeurt voor commerciële doeleinden. De gegevens die geregistreerd worden zijn in beide gevallen echter privacygevoelig en zullen door consumenten op verschillende wijzen ervaren worden, met een wisselend effect op hun privacybeleving. Ook omgekeerd zullen mensen die zich meer zorgen maken over hun privacy, de verschillende technologieën anders beoordelen.

## 3.6 INVLOED & CONTROLE

Ook de mate van invloed die burgers zelf uit kunnen oefenen op de diensten die zij gebruiken en de gegevens die daarbij verwerkt worden, is van belang voor de beleving van privacy. Vaak is onduidelijk welke gegevens worden verwerkt en voor welke doelen deze worden gebruikt, waardoor de consument ook geen beeld heeft van de mogelijke impact op zijn privacy. Hier wordt privacy dus gekoppeld aan vertrouwen en transparantie. Om te kunnen bepalen of mensen het gevoel hebben voldoende invloed uit te kunnen oefenen op het gebruik van hun gegevens, zullen we de respondenten eerst vragen in welke mate zij behoefte hebben aan deze controle.[10] Vervolgens zullen we hen vragen in welke mate zij ook daadwerkelijk het gevoel hebben dat zij die controle kunnen uitoefenen. Daarnaast kijken we of de behoefte aan controle en de mate waarin men controle ervaart ook verband houdt met de algemene beleving van privacy.

Men kan zelf invloed uitoefenen op de bescherming van persoonsgegevens, door zijn of haar gedrag aan te passen. Zo kan men invloed uitoefenen op het gebruik van gegevens door het aanpassen van instellingen op sociale media om te bepalen welke informatie met wie gedeeld mag worden, gebruik van wisselende wachtwoorden of het niet invullen van gevraagde gegevens. Ook kan men technieken inzetten om gegevens te beschermen. Denk bijvoorbeeld aan het installeren van beveiligingssoftware of *ad blockers*. Of het gebruik van een bepaalde browser die meer mogelijkheden biedt voor anoniem surfen en het installeren van add-ons die cookies of advertenties blokkeren. In de VS heeft inmiddels 86% van de internetgebruikers dit soort maatregelen genomen om surveillance door overheden of andere organisaties tegen te gaan.[11] Dat is een zeer hoog percentage. Dat wijst erop dat mensen vooral graag controle houden over wie er toegang heeft tot hun gegevens. We zullen onderzoeken of dit voor Nederlandse internetgebruikers hetzelfde is.

---

10 Privacy wordt in de literatuur vaak uitgelegd als controle over wie toegang heeft tot welke informatie. Zie bijvoorbeeld: A. Westin (1967) Privacy and Freedom, ; D. Solove (2008) Understanding Privacy, The George Washington University Law School Public Law and Legal Theory Working Paper No. 420 Legal Studies Research Paper No. 420.

11 PEW Research Center (2013). Anonymity, Privacy, and Security Online.

De vraag is echter of het daadwerkelijk gebruik maken van technische tools om privacy beter te beschermen (zoals het installeren van beveiligingssoftware op computers) ook echt samenhangt met gedrag dat gericht is op privacybescherming, of dat hier ook sprake is van een privacy paradox. Zijn mensen die privacybeschermende software hebben geïnstalleerd ook voorzichtiger in het delen van hun gegevens?

Er zijn situaties waarin het weigeren om gegevens te delen onmogelijk is of moeilijk wordt gemaakt, omdat er geen keuzevrijheid lijkt te bestaan. Consumenten voelen zich soms gedwongen om bepaalde gegevens te verstrekken, ook al willen ze dit niet. Een bekend voorbeeld hiervan is het accepteren van cookies op websites, waarmee het surfgedrag van internetgebruikers gevolgd kan worden. Niet iedereen wil daar toestemming voor geven, maar het weigeren van cookies leidt soms tot een beperkte functionaliteit van een website of zelfs helemaal geen toegang. Omdat iemand toch toegang wil tot bepaalde content, is er daarom geen sprake van een echte vrije keuze.

Een andere vorm van keuzebeperking is zogeheten *peer pressure*.[12] Het is lastiger om niet mee te doen met een sociaal netwerk (bijvoorbeeld Facebook) als iedereen in je omgeving dat wel doet. Veel mensen hebben tegen hun zin een Facebook account, omdat ze bang zijn anders te veel te missen van het sociale leven van hun vrienden. Zo worden uitnodigingen voor verjaardagen regelmatig alleen nog via Facebook verspreid. Niet meedoen betekent dan dus automatisch niet uitgenodigd worden. We zullen in de survey navragen of ook in Nederland mensen – ondanks hun zorgen over hun privacy – inderdaad gebruik maken van bepaalde diensten en sociale media vanwege druk uit hun omgeving.

## 3.7 AWARENESS

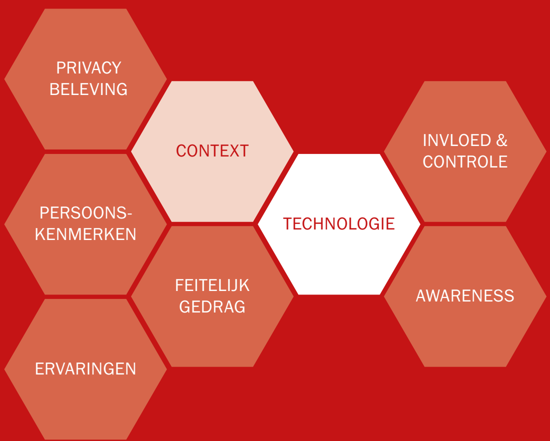
Tot slot is het van belang om inzicht te verkrijgen in het algemene niveau van privacybewustzijn onder de Nederlandse bevolking. In hoeverre zijn mensen op de hoogte van de mogelijke consequenties voor hun privacy door het gebruik van hun persoonsgegevens door derden? Denkt men wel eens na over de gevolgen van het gebruik van internet voor de bescherming van persoonsgegevens? En spreekt men er wel eens over met zijn of haar omgeving? De verwachting is dat mensen die zich veel bezig houden met de bescherming van hun persoonsgegevens en een kritische houding hebben ten aanzien van het gebruik van deze gegevens, hier ook meer met hun omgeving over spreken.

Ook zijn we benieuwd naar de kennis die mensen hebben over het maatschappelijk veld dat zich bezighoudt met de bescherming van persoonsgegevens. Bekendheid met organisaties die zich inzetten voor bescherming van privacy zegt iets over de betrokkenheid van mensen bij het onderwerp. De bekendheid met organisaties kan echter op twee wijzen worden uitgelegd: er is vertrouwen, omdat er organisaties mee bezig zijn, of er is geen vertrouwen, omdat dergelijke organisaties nodig zijn. Binnen Nederland gaat het om de digitale burgerrechtenorganisaties Bits of Freedom en Privacy First. Op Europees niveau wordt vooral uitleg gegeven over de toepassing van privacyregelgeving door de Artikel 29 Werkgroep. Internationaal zijn Electronic Frontier Foundation (EFF), Privacy International en het Electronic Privacy Information Center (EPIC) het bekendst. We zullen de respondenten vragen in hoeverre zij bekend zijn met deze organisaties, die zich beijveren voor de bescherming van hun privacy en persoonsgegevens.

---

12 boyd, d. (2008) “Why Youth Heart Social Network Sites: The Role of Networked Publics in Teenage Social Life.” *Youth, Identity, and Digital Media*. Edited by David Buckingham. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA: The MIT Press, pp. 119–142. doi: 10.1162/dmal.9780262524834.119

# HOE VOELT U ZICH **BIJ HET GEBRUIK VAN TECHNOLOGIE DIE UW INTERNETVERKEER MONITORT?**



# 4 RESULTATEN
## DE BELEVING VAN PRIVACY IN NEDERLAND

DIT HOOFDSTUK BEVAT DE RESULTATEN VAN DE SURVEY DIE IS UITGEZET ONDER EEN REPRESENTATIEVE STEEKPROEF VAN DE NEDERLANDSE BEVOLKING. WE BESPREKEN HIER DE UITKOMSTEN VAN HET ONDERZOEK EN DE RELATIE VAN DE ZEVEN FACTOREN MET DE PRIVACYBELEVING IN NEDERLAND.

We beginnen met een beschrijving van de steekproef: welk type mensen heeft aan dit onderzoek deelgenomen? Ook geven we in deze beschrijving toelichting op de sterkte van de significante verbanden die we hebben gevonden. Daarna schetsen we een beeld van de algemene beleving van privacy onder de deelnemers aan het onderzoek. Hoe beleeft de gemiddelde Nederlander zijn privacy? Hoe denkt hij of zij over het beschermen en delen van persoonsgegevens? Vervolgens zal voor de zeven genoemde factoren (persoonskenmerken, ervaringen, feitelijk gedrag, context, technologie, invloed & controle en awareness) vastgesteld worden wat deze over de beleving van privacy zeggen.

### 4.1 BESCHRIJVING VAN DE STEEKPROEF

De vragenlijst voor deze monitor is afgenomen tussen 7 en 11 januari 2015. In Tabel 1 is de dataset beschreven die hieruit is ontstaan. De dataset is representatief voor de Nederlandse bevolking op de factoren leeftijd, geslacht en regio waarin de respondenten wonen. In totaal is de vragenlijst ingevuld door 1066 respondenten, waarvan 47,9% mannen en 52,1% vrouwen.
De grootste groep respondenten valt in de leeftijdscategorie tussen de 35 en 54 jaar (43,4%).
De meeste respondenten wonen in de regio Noord Holland, Zuid Holland en Utrecht (exclusief Amsterdam, Rotterdam en Den Haag), namelijk 30,1%. Het grootste deel van de respondenten heeft een gemiddeld opleidingsniveau (44,6%). Op de vraag waar men zich zou plaatsen op een schaal van links (1) tot rechts (10) in het politiekspectrum, scoren de respondenten een 5,6 gemiddeld, dus in het midden van het politieke spectrum. Op de vraag of de respondenten de meeste mensen in het algemeen te vertrouwen zijn – op een schaal van 1 (je kunt niet voorzichtig genoeg zijn) tot 10 (de meeste mensen zijn te vertrouwen), scoren de respondenten gemiddeld een 5,4. De respondenten hebben dus niet heel veel, maar ook niet heel weinig algemeen vertrouwen in de ander. Daarnaast is specifiek gevraagd naar het vertrouwen in de Nederlandse overheid, daarop scoren de respondenten eveneens een 5,4 op dezelfde vertrouwensschaal. Daarbij geeft de grootste groep (20,5%) een 7 aan hun vertrouwen in de overheid.

*Tabel 1 Beschrijving van de data*

| VARIABELE | AANTAL | PERCENTAGE |
|---|---|---|
| Aantal respondenten | 1066 | 100% |
| Vrouw | 555 | 52.1% |
| Man | 511 | 47.9% |
| Lager opgeleid (Basisonderwijs, LBO, VBO, LTS, LHNO, VMBO, MAVO, VMBO-t, MBO-kort) | 255 | 23.9% |
| Midden opgeleid (MBO, MTS, MEAO, HAVO, VWO, Gymnasium) | 475 | 44.6% |
| Hoger opgeleid (HBO, HEAO, PABO, HTS, Universiteit) | 333 | 31.2% |
| Leeftijd 18-34 | 272 | 25.5% |
| Leeftijd 35-54 | 462 | 43.4% |
| Leeftijd 55-74 | 332 | 31.1% |
| Regio Randstad (Amsterdam, Rotterdam, Den Haag) | 132 | 12.4% |
| Regio Noord-Holland, Zuid-Holland, Utrecht (excl. Randstad) | 321 | 30.1% |
| Regio Noord Nederland (Groningen, Friesland, Drenthe) | 122 | 11.4% |
| Regio Oost Nederland (Overijssel, Gelderland, Flevoland) | 215 | 20.2% |
| Regio Zuid Nederland (Zeeland, Noord Brabant, Limburg) | 276 | 25.9% |

De significante ($p < 0.01$) correlaties – of samenhangen tussen twee variabelen – die we in dit onderzoek hebben aangetroffen, blijken allemaal relatief zwak te zijn (tussen de 0.1 en 0.2 op een schaal van 0 tot 1). Correlaties duiden er op dat er wel een relatie bestaat tussen twee variabelen, maar niet dat deze verklarend zijn voor elkaar. Dat betekent bijvoorbeeld dat iemands leeftijd wel een relatie heeft met hoe hij of zij over iets denkt, maar het zegt niet dat de leeftijd verklaart dat hij zo denkt. Waar we nader in gaan op correlaties tussen twee variabelen, zullen we steeds aangeven hoe sterk de aangetroffen correlaties of samenhangen tussen twee variabelen zijn (aangeduid met een Pearsons r).

## 4.2 ALGEMENE BELEVING VAN PRIVACY: DELEN EN BESCHERMEN VAN PERSOONSGEGEVENS

De kern van deze monitor draait om de beleving van privacy door Nederlanders, in het bijzonder op het internet en bij online dienstverlening waar persoonsgegevens gedeeld worden. Om een beeld te krijgen van die privacybeleving, is in de survey een aantal vragen gesteld over het belang dat men hecht aan de bescherming van persoonsgegevens en de houding die men heeft tegenover het delen van gegevens op het internet. In Figuur 1 is het algemene beeld van die privacybeleving weergegeven.

Van de respondenten is 82,5% het ermee eens of helemaal mee eens dat het belangrijk is dat hun persoonsgegevens beschermd worden. Slechts 4,4% van de respondenten is het hier niet mee eens en vindt het niet van belang om persoonsgegevens te beschermen. Ongeveer 3 op de 10 respondenten vindt het normaal in een moderne maatschappij om informatie te delen (30,5%), terwijl 43,3% daarover twijfelt en het 'noch eens, noch oneens' is met de stelling. De meeste respondenten vinden dat het geven van persoonlijke informatie via internet een onderwerp is waar aandacht voor moet zijn in de maatschappij (71,2% is het hiermee eens of helemaal eens). Met andere woorden: zowel de mensen die geneigd zijn persoonsgegevens te delen als de mensen die geneigd zijn dit niet te doen, vinden het onderwerp 'geven van persoonlijke informatie via het Internet' van belang. En 14,9% van de respondenten vindt het ook geen probleem om persoonlijke

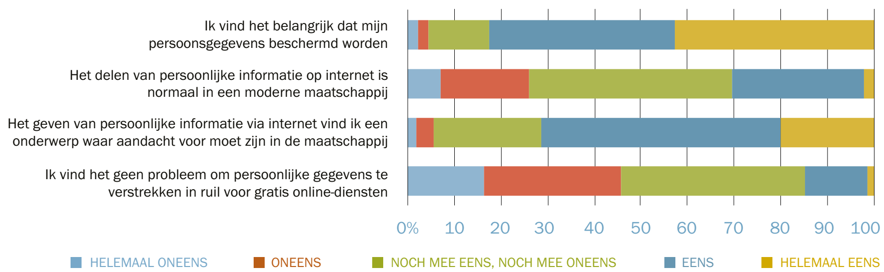
gegevens te verstrekken in ruil voor gratis online diensten. De overige 85,1% is het 'noch eens, noch oneens' met de stelling (39,5%) of zelfs oneens of helemaal oneens (45,6%)en vindt het verstrekken van persoonlijke gegevens in ruil voor gratis diensten wel een probleem.

Over het algemeen wordt dus het beschermen van persoonsgegevens van belang geacht, evenals het maatschappelijk debat over deze kwesties. Daarnaast is men terughoudend bij het delen van informatie op het internet in ruil voor gratis diensten en is men nog enigszins ambivalent als het gaat om het delen van informatie op het internet als gegeven van de moderne maatschappij.

*Figuur 1*

**ALGEMENE OPINIE OVER DE BESCHERMING VAN PERSOONSGEGEVENS**

GEEF VOOR DE VOLGENDE UITSPRAKEN AAN IN HOEVERRE U HET HIER MEE EENS OF ONEENS BENT




## 4.3 DE ZEVEN FACTOREN IN RELATIE TOT PRIVACYBELEVING IN NEDERLAND

### 4.3.1 PERSOONSKENMERKEN

Uit de beschrijving van de steekproef bleek al dat de survey is afgenomen onder verschillende groepen mensen. Zo kunnen we onderzoeken of de leeftijd of het geslacht van de respondenten van invloed is op hun algemene privacybeleving. Vinden mannen het bijvoorbeeld meer vanzelfsprekend om hun gegevens te delen dan vrouwen? Of vinden jongeren (van de 'Facebookgeneratie') het minder problematisch om hun gegevens te delen in ruil voor gratis diensten dan dat bijvoorbeeld ouderen dit vinden? Voor een aantal demografische kenmerken, te weten leeftijd, geslacht en opleidingsniveau, hebben we onderzocht of er significante verschillen bestaan.

**Demografische kenmerken**

Uit de analyse blijkt dat er geen significante verschillen bestaan tussen mannen en vrouwen: ze blijken privacy even belangrijk te vinden. Ook het opleidingsniveau blijkt geen relatie te hebben met de beleving van privacy: lager en hoger opgeleiden vinden de bescherming van hun persoonsgegevens even belangrijk.

Wanneer we kijken naar de leeftijd van de respondenten en het belang dat zij hechten aan hun privacy, dan valt op dat jongvolwassenen (tussen de 18 en 34 jaar) de bescherming van persoonsgegevens significant minder belangrijk vinden dan de oudere respondenten (-.146) en dat zij het delen van gegevens op het internet in lichte mate een normaler verschijnsel vinden in de huidige maatschappij (.115). Ook vinden zij het maatschappelijk gesprek over het delen van informatie op internet iets minder van belang (-.132), terwijl oudere volwassenen (55 – 74 jaar) het wel van

belang vinden (.128). Tot slot valt op dat oudere volwassenen (55-74 jaar) iets meer moeite hebben met het delen van persoonsgegevens op het internet in ruil voor gratis diensten (-.130). Voor de andere leeftijdscategorieën is hier geen significante relatie gevonden.

Eén van de stellingen uit de theorie was dat naarmate jongeren (van de Facebookgeneratie) ouder worden, ze ook kritischer na gaan denken over hun privacy. Of dit effect over tijd daadwerkelijk bestaat is helaas nog niet vast te stellen. Wel wordt duidelijk dat jongeren het beschermen van hun persoonsgegevens iets minder belangrijk vinden en het normaler vinden om hun gegevens te delen. En dat ouderen hier anders over denken en de bescherming van persoonsgegevens belangrijker vinden. Mogelijk dat een studie over langere tijd meer duidelijkheid geeft over de groei in het besef van privacy.

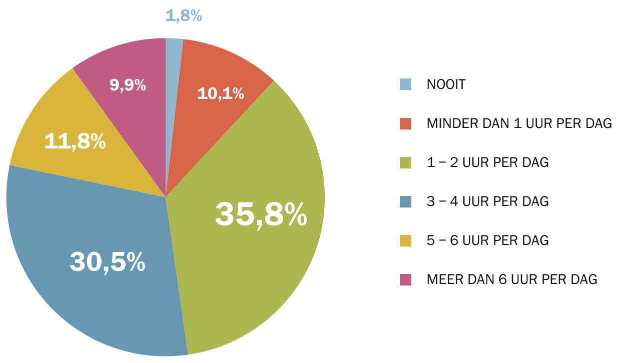
**Intensiteit van internetgebruik**

Een andere veronderstelling was dat de intensiteit van het internetgebruik van invloed is op de algemene privacybeleving. Hoe meer tijd mensen op het internet doorbrengen, hoe meer om persoonsgegevens gevraagd wordt en des te meer zij gewend zouden zijn geraakt aan het delen van deze informatie. We hebben de respondenten allereerst gevraagd hoeveel tijd zij op het internet doorbrachten, exclusief het internetgebruik op het werk, maar inclusief gebruik van mobiel internet. Daar kwam het volgende beeld uit naar voren (zie Figuur 2): de grootste groep respondenten (35,8%) zegt 1 tot 2 uur per dag het internet te gebruiken, 30,5% gebruikt het 3 tot 4 uur per dag. Een kleine groep van 9,9% van de respondenten geeft aan meer dan 6 uur per dag gebruik te maken van internet voor privédoeleinden[13].

*Figuur 2*

**GEMIDDELD GEBRUIK INTERNET VOOR PRIVÉDOELEINDEN**

HOEVEEL UUR PER DAG MAAKT U GEMIDDELD GEBRUIK VAN HET INTERNET VOOR PRIVÉDOELEINDEN (HIERONDER VALT OOK MOBIEL INTERNET EN GEBRUIK VAN APPS)?




13 Bij deze cijfers moet opgemerkt worden dat respondenten vaak onderschatten hoeveel tijd ze daadwerkelijk internetten of televisiekijken. Het daadwerkelijke gebruik zal vermoedelijk iets hoger liggen.

De verwachting was dat mensen die veel op het internet surfen, een andere houding zouden hebben ten aanzien van privacy dan mensen die minder actief online zijn. Hier blijkt echter geen significant verband te bestaan, wat betekent dat niet kan worden aangetoond dat de hoeveelheid uren die iemand per dag online is een significante relatie heeft met het denken over de bescherming van persoonsgegevens.

### 4.3.2 ERVARINGEN

In de theorie stelden we dat eerdere ervaringen die mensen hebben gehad, mogelijk voorspellend zijn voor de privacybeleving van mensen. Mensen die zich er van bewust zijn dat zij slachtoffer zijn geweest van diefstal of misbruik van persoonsgegevens of van identiteitsfraude, zouden meer belang hechten aan goede bescherming van persoonsgegevens om herhaling van deze ervaring te voorkomen. In de survey is gevraagd naar eerdere ervaringen met verlies of misbruik van persoonsgegevens en ervaringen met identiteitsfraude.

**Ervaringen met verlies of diefstal van persoonsgegevens**

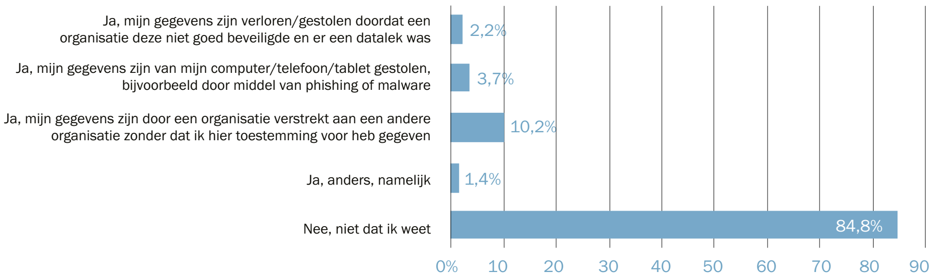
Op de vraag of ze ooit te maken hebben gehad met verlies of diefstal van persoonsgegevens, antwoord 15,2% van de respondenten bevestigend. In Figuur 3 is terug te zien met welk type incidenten zij te maken hebben gehad: het ging bij de meeste respondenten (10,2%) om een incident waarbij de organisatie die zijn of haar gegevens verwerkt had, deze ook aan een andere organisatie heeft doorgegeven zonder de respondent om toestemming te vragen. Andere incidenten die de respondenten hebben genoemd, zijn het vrijgeven van gegevens door de belastingdienst zonder toestemming en het doorspelen van informatie over iemands ouder zonder toestemming. Dit type incidenten waarbij persoonsgegevens verloren of gestolen worden, deed zich in 52,4% van de gevallen voor in het afgelopen jaar.

Tegenover deze slachtoffers staan 84,8% van de respondenten die aangeven geen slachtoffer te zijn geweest van verlies of diefstal van persoonsgegevens. Mogelijk ligt dit percentage in werkelijkheid iets lager: de respondenten kunnen slachtoffer zijn geweest van verlies of diefstal van persoonsgegevens zonder dit te weten. Het verlies of de diefstal kan hebben plaatsgevonden bij een organisatie die de gegevens hebben opgeslagen.

*Figuur 3*

**ERVARING VERLIES OF DIEFSTAL PERSOONSGEGEVENS**

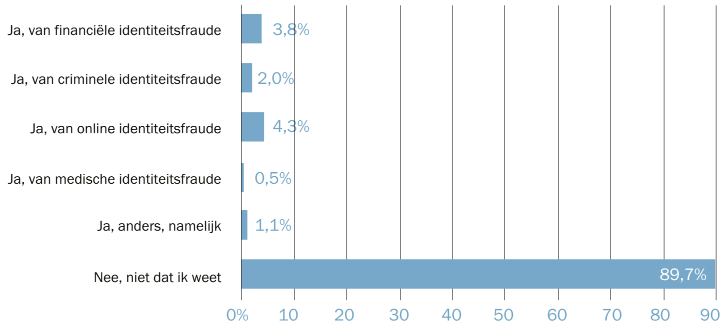
HEEFT U VOOR ZOVER U WEET OOIT TE MAKEN GEHAD MET VERLIES OF DIEFSTAL VAN UW PERSOONSGEGEVENS?



**Ervaringen met identiteitsfraude**
Een andere vorm waarbij persoonsgegevens onrechtmatig worden gebruikt is identiteitsfraude. Dit houdt in dat iemand de persoonsgegevens van een andere persoon gebruikt en zich voor die ander uitgeeft, om vervolgens contact te zoeken met derden (ook wel 'catphishing' genoemd), criminele activiteiten te ondernemen of aankopen te doen.

De grote meerderheid van de respondenten (89,7%) geeft aan niet bewust te zijn van identiteitsfraude. Dat houdt in dat 10,3% – ongeveer 1 op de 10 mensen – aangeeft hier wel slachtoffer van te zijn geweest of zich hier van bewust te zijn. In Figuur 4 is terug te zien met welk type incidenten deze respondenten te maken hebben gehad. Het gaat voornamelijk om online identiteitsfraude, (waarbij iemand anders zich online uitgeeft voor die persoon) of financiële identiteitsfraude (3,8%). Medische identiteitsfraude lijkt niet vaak voor te komen (0,5%). Andere vormen van identiteitsfraude die door respondenten worden genoemd zijn misbruik van persoonsgegevens bij langdurige ziekte, het afsluiten van verzekeringen op iemand anders zijn naam of het opgeven van andermans persoonsgegevens bij een verkeersboete. Dit type incidenten, waarbij fraude wordt gepleegd met iemands identiteit op basis van onrechtmatig verkregen persoonsgegevens, heeft zich in 39,7% van de gevallen in het afgelopen jaar voorgedaan.

*Figuur 4*
**ERVARING IDENTITEITSFRAUDE**
BENT U VOOR ZOVER U WEET WELEENS HET SLACHTOFFER GEWEEST VAN IDENTITEITSFRAUDE?




Wanneer we kijken of deze eerdere ervaringen inderdaad een relatie hebben met de algemene beleving van privacy, dan blijkt er alleen een zwak verband te bestaan tussen het slachtoffer zijn van verlies of diefstal van gegevens en het van belang vinden dat er in de maatschappij over bescherming van persoonsgegevens wordt gesproken (.131).

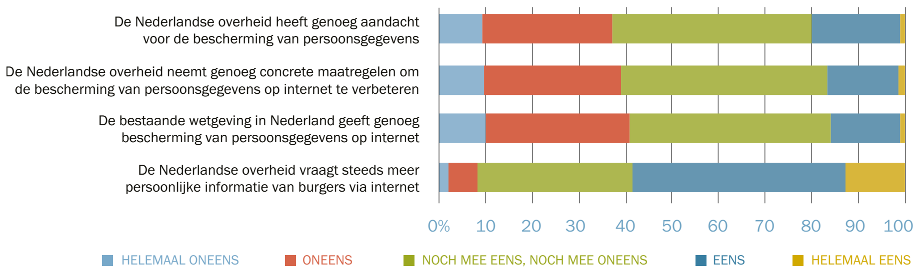
**Optreden van overheden**
Naast eerdere ervaringen, is de respondenten ook gevraagd hoe zij het optreden van de overheid en de ingestelde wet- en regelgeving beoordelen (zie Figuur 5). Wat allereerst opvalt bij deze stellingen is dat vaak het antwoord 'noch mee eens, noch mee oneens' gekozen wordt. Op de vraag of zij vinden dat de overheid voldoende aandacht heeft voor de bescherming van persoonsgegevens, kiest 42,5% van de respondenten voor deze neutrale antwoordcategorie. Dit antwoord wordt ook vaak gekozen bij de stelling dat 'de overheid genoeg concrete maatregelen treft om de bescherming van persoonsgegevens te verbeteren' (44,4%),'de bestaande wetgeving voldoende

bescherming biedt' (43,4%). Men lijkt het moeilijk te vinden om hier een oordeel over te vellen. Dit kan komen doordat men onvoldoende geïnformeerd is, of omdat men er geen volmondig ja of nee op kan of wil geven. Er lijkt overigens meer consensus te bestaan over de hoeveelheid informatie die de overheid vraagt: 58,5% is het er mee eens of helemaal mee eens dat 'de Nederlandse overheid steeds meer informatie vraagt van burgers via het internet'.

*Figuur 5*

**OPINIE OVER OPTREDEN OVERHEID BIJ BESCHERMING PERSOONSGEGEVENS**

GEEF VOOR DE VOLGENDE UITSPRAKEN AAN IN HOEVERRE U HET HIER MEE EENS OF ONEENS BENT




4.3.3 FEITELIJK GEDRAG

Bij de persoonskenmerken zagen we al dat de meeste respondenten tussen 1-2 uur (35,8%) of 3-4 uur (30,5%) per dag op het internet doorbrengen voor privédoeleinden. Daarnaast hebben we ook gevraagd welke diensten zij op dat moment gebruiken.

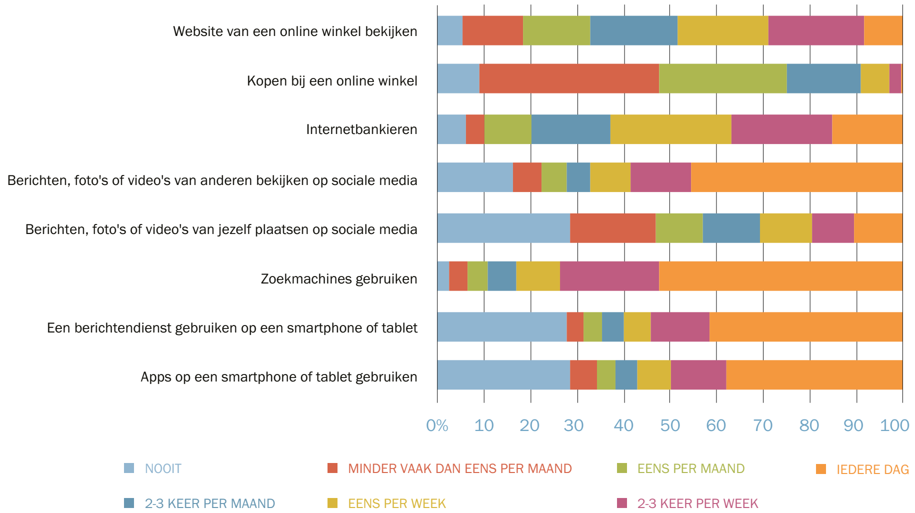
**Activiteiten online**

In Figuur 6 is een overzicht te zien van verschillende online activiteiten en de frequentie waarmee de respondenten deze activiteiten in de afgelopen 12 maanden hebben ondernomen. Van een aantal activiteiten geven de respondenten aan dit vrijwel dagelijks of in ieder geval een aantal keren per week te doen: een zoekmachine gebruiken (73,5%), berichten, foto's of video's van anderen op sociale media bekijken (58,3%) of een bericht sturen via een berichtendienst als WhatsApp (54,1%). Hoewel de respondenten aangeven regelmatig berichten, foto's of video's van anderen te bekijken op sociale media, plaatst een veel kleiner percentage ook daadwerkelijk zelf met regelmaat iets op sociale media (19,5%) en zelfs 28,5% van de respondenten helemaal nooit. Tot slot valt op dat berichtendiensten als WhatsApp een grote groep dagelijkse gebruikers kennen (41,5% van de respondenten), terwijl daarnaast ruim een kwart (28%) aangeeft dit type diensten nooit te gebruiken.

*Figuur 6*

**DOELGEBRUIK VAN INTERNET IN DE AFGELOPEN 12 MAANDEN**

KUNT U OVER DE VOLGENDE ACTIVITEITEN ZEGGEN HOE VAAK U DIT IN DE AFGELOPEN 12 MAANDEN HEEFT GEDAAN?




In de theorie introduceerden we reeds de privacy paradox: hoe mensen over privacy en de bescherming van persoonsgegevens denken, komt niet altijd overeen met het gedrag dat ze vertonen. Zo kan iemand zeggen privacy belangrijk te vinden, maar vervolgens veel persoonsgegevens achterlaten op zijn of haar profiel op Facebook.

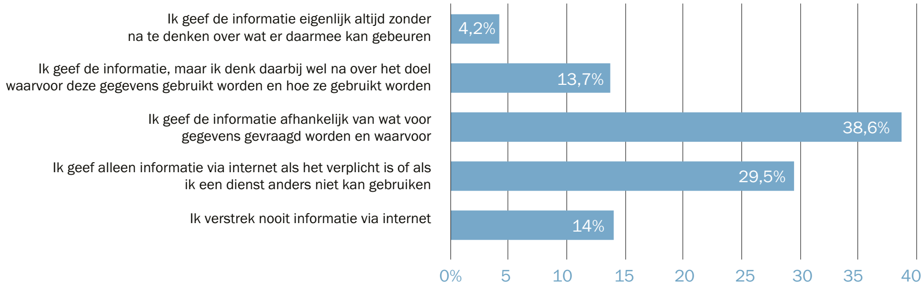
**Bereidheid om informatie te geven**

In de survey is de respondenten gevraagd wat zij doen als er op het internet om persoonlijke informatie wordt gevraagd (zie Figuur 7). Slechts 4,2% van de respondenten geeft aan de informatie zonder na te denken te geven. Het merendeel van de respondenten zegt alleen informatie te geven als duidelijk is waarom dit nodig is (38,6%) of alleen als het verplicht is of nodig is om de dienst te kunnen gebruiken (29,5%). Van de respondenten geeft 14% aan nooit persoonlijke informatie te delen. Het merendeel van de respondenten deelt zijn gegevens dus wel, maar is terughoudend in de hoeveelheid en het type informatie dat ze prijsgeven. Dit is opvallend en lijkt er op te wijzen dat het deelnemen aan bepaalde diensten belangrijker wordt gevonden dan het beschermen van de gegevens.

*Figuur 7*

**OMGANG MET VERZOEKEN VOOR HET VERSTREKKEN VAN PERSOONLIJKE INFORMATIE**

WAT DOET U ALS U VIA INTERNET WORDT GEVRAAGD OM PERSOONLIJKE INFORMATIE OVER UZELF TE GEVEN?




Zoals te verwachten is, zijn de respondenten die het normaal vinden om informatie te delen iets meer geneigd hun gegevens prijs te geven (.212). Dit geldt ook voor de respondenten die hun gegevens verstrekken in ruil voor gratis diensten (.219). Ook blijkt dit voor alle typen diensten significant te zijn: de mensen die makkelijker gegevens verstrekken blijken dit voor alle typen diensten te doen die in Figuur 6 genoemd worden. Het verband is echter ook hier relatief zwak (tussen de .110 en .158). Het blijkt wel iets sterker te zijn voor het kopen in webwinkels (.188) en zoekmachines (.182), maar dit komt mogelijk doordat dit sowieso meer gebruikte diensten zijn (en dus de groep gebruikers iets groter is).

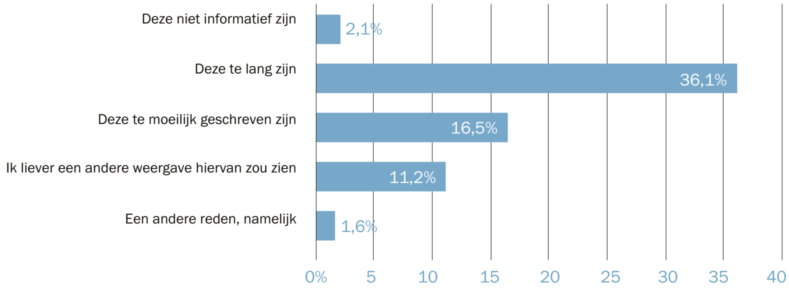
**Algemene voorwaarden en privacyreglementen lezen**

Ander gedrag waaruit blijkt dat men belang hecht aan privacy en bescherming van persoonsgegevens is het lezen van algemene voorwaarden en/of het privacyreglement van een dienst (bijvoorbeeld een app), voordat men gebruik gaat maken van de dienst. Er is gevraagd of men deze voorwaarden en reglementen leest of niet. Op deze vraag antwoordt 49,3% van de respondenten dat ze dit meestal doen. Deze percentages komen overeen met de percentages in Australië (49%) en Canada (50%) die in de theorie genoemd werden. Van de mensen die deze voorwaarden lezen, vindt 39,2% dat deze meestal voldoende informatie geven, 43,5% vindt dat de voorwaarden en reglementen niet genoeg informatie geven en 16.9% geeft aan dit niet te weten (naast 0,4% die ‘niet van toepassing’ heeft geantwoord).

Aan de respondenten die hebben aangegeven de algemene voorwaarden en/of het privacyreglement meestal niet te lezen, hebben we gevraagd wat de redenen hiervoor zijn. Enkele mogelijke redenen zijn voorgegeven. Het resultaat hiervan is in Figuur 8 te zien. Veruit de grootste groep geeft aan de voorwaarden niet te lezen omdat ze te lang zijn (53,5%). Daarnaast wordt gezegd dat ze te moeilijk zijn (24,5%) of beter anders weergegeven kunnen worden (16,6%).

*Figuur 8*

**REDENEN VOOR HET NIET LEZEN VAN ALGEMENE VOORWAARDEN OF PRIVACY STATEMENTS** IK LEES DE ALGEMENE VOORWAARDEN OF PRIVACY STATEMENTS NIET, OMDAT...




Ook hier wordt de privacy paradox weer zichtbaar: hoewel men het van belang acht dat persoonlijke gegevens goed beschermd worden en men liever niet onnodig informatie prijsgeeft, leest de helft van de respondenten de algemene voorwaarden – waarin meer informatie gegeven zou moeten worden over de omgang met persoonsgegevens – niet. Kennelijk kost dat in verhouding te veel moeite, omdat het veel leeswerk (tijd) inhoudt. Bovendien kan er niet altijd de benodigde informatie uit gehaald worden.

### 4.3.4 CONTEXT

De bescherming die mensen verlangen voor hun persoonsgegevens, hangt volgens de theorie in grote mate af van de context waarin gegevens gevraagd worden. De houding ten aanzien van de wijze waarop gegevens beschermd moeten worden, kan al naar gelang de instelling of persoon die de gegevens verwerkt verschillen. Deze houding hebben wij vertaald in het vertrouwen dat de respondenten hebben in de wijze waarop organisaties de gegevens verwerken. De verwachting was dat een groter vertrouwen in een organisatie er toe leidt dat de bescherming van persoonsgegevens als beter wordt ervaren.

**Vertrouwen in organisaties**

We hebben de respondenten gevraagd in hoeverre zij bepaalde organisaties die hun persoonsgegevens verwerken vertrouwen als het gaat om het beschermen van de gegevens en het enkel gebruiken van de gegevens voor het vooraf bepaalde doel. Er is daarbij onderscheid gemaakt naar verschillende typen bedrijven en sectoren. De resultaten zijn terug te lezen in Figuur 9. In de figuur valt op dat het vertrouwen in de verschillende organisaties sterk uiteen loopt. De politie geniet het meeste vertrouwen: 45,5% van de respondenten geeft aan hier veel tot zeer veel vertrouwen in te hebben. Ook de Belastingdienst (43,2%), werkgevers (39,2%) en instellingen in de gezondheidszorg (42,6%) wordt veel tot zeer veel vertrouwen toegedicht. Veruit het minste vertrouwen heeft men in de wijze waarop sociale media gegevens beschermen en inzetten voor de afgesproken doelen: 74,8% van de respondenten geeft aan hier weinig tot zeer weinig vertrouwen in te hebben. Andere organisaties die weinig vertrouwen genieten zijn webwinkels (58,4% heeft hier weinig tot zeer weinig vertrouwen in), goede doelenorganisaties (50,5%) en marktonderzoeksbureaus (50,5%). Dit type organisaties is zeer gebaat bij het verzamelen en gebruiken van persoonsgegevens. Hier tegenover staan organisaties die meer belang hebben bij bescherming van persoonsgegevens, zoals instellingen in de gezondheidszorg. Deze organisaties worden dan ook meer vertrouwd in het beschermen en doelmatig gebruiken van persoonsgegevens.

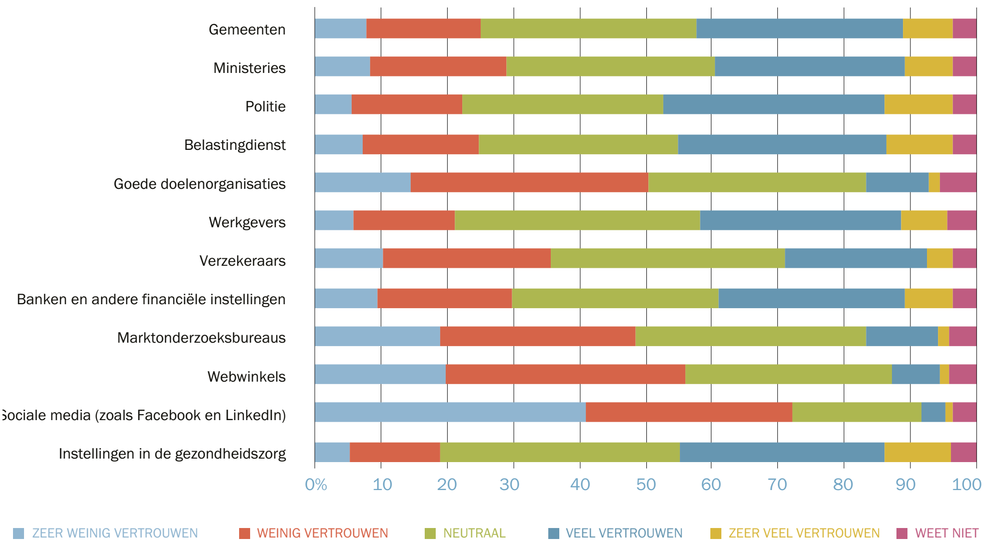
Een ander onderscheid dat hierbij opvalt, is dat de organisaties die minder vertrouwd worden primair actief zijn in de online sfeer, terwijl de organisaties die meer vertrouwd worden primair actief zijn in de fysieke wereld of de offline sfeer.

Bij de vragen die gerelateerd zijn aan vertrouwen in organisaties, valt op dat respondenten vaker voor de antwoordcategorie 'neutraal' hebben gekozen. Dit kan er op wijzen dat men geen goed beeld heeft of dat men niet overtuigd is dat hun gegevens wél goed beschermd worden door deze organisaties. Ook heeft bijna 4% van de respondenten 'weet niet' geantwoord op deze items, wat gemiddeld meer is dan op de andere vragen in de survey. Mogelijk vond men het moeilijk om te beoordelen hoe organisaties hier mee omgaan. Een opvallende uitschieter bij deze "weet niet" categorie zijn de goede doelenorganisaties: daarbij geeft 5,4% van de respondenten aan niet te weten hoe zij omgaan met de toepassing en de bescherming van persoonsgegevens.

*Figuur 9*

**VERTROUWEN IN BESCHERMING PERSOONSGEGEVENS DOOR ORGANISATIES**

GEEF VOOR ONDERSTAANDE (TYPEN) ORGANISATIES AAN HOEVEEL VERTROUWEN U ER IN HEEFT DAT ZIJ PERSOONSGEGEVENS GOED BESCHERMEN EN ALLEEN VOOR VOORAF BEPAALDE DOELEN GEBRUIKEN




Als we dit vertrouwen in organisaties afzetten tegen het algemene privacygevoel dat mensen hebben, dan blijken alleen de verbanden voor het vertrouwen in commerciële partijen zwak maar significant te zijn: de respondenten die de bescherming van persoonsgegevens belangrijk vinden, hebben minder vertrouwen in marktonderzoeksbureaus (-.123), webwinkels (-.146) en sociale media (-.212).

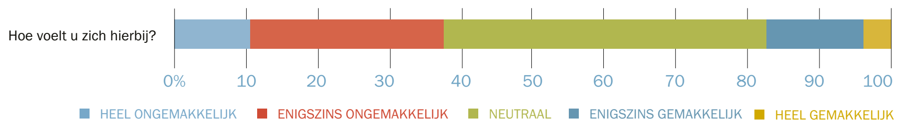
Wanneer we kijken naar de respondenten die hebben aangegeven het normaal te vinden om gegevens te delen op het internet, dan blijken er meerdere significante correlaties te bestaan – al zijn deze verbanden relatief zwak. Deze respondenten hebben voornamelijk vertrouwen in ministeries (.228), de politie (.209), werkgevers (.216), verzekeraars (.209) en banken (.215).

De respondenten die hebben aangegeven dat er aandacht moet zijn voor bescherming van persoonsgegevens, geven aan op dat terrein minder vertrouwen te hebben in sociale media (-.247) en webwinkels (-.177). Er is ook een significante correlatie voor het vertrouwen in verzekeraars (-.126) en marktonderzoeksbureaus (-.123), maar deze verbanden zijn bijzonder zwak.

**Persoonsgegevens ruilen voor gratis diensten**
Tot slot hebben we de respondenten gevraagd in hoeverre zij bereid zijn om persoonsgegevens te delen in ruil voor gratis diensten. De respondenten is een situatie voorgelegd, waarbij commerciële partijen zoals Hotmail, Apple, Microsoft of Google gratis diensten leveren in ruil voor persoonsgegevens, die ze doorverkopen aan adverteerders om hun advertentieaanbod beter af te stemmen op de gebruiker. De respondenten is gevraagd hoe gemakkelijk of ongemakkelijk ze zich daarbij voelen. In Figuur 10 is te zien dat 37,7% van de respondenten zich hier enigszins ongemakkelijk of heel ongemakkelijk bij voelt. Een grote groep respondenten antwoordt 'neutraal' (44,9%). Een veel kleinere groep van 17,4% van de respondenten geeft aan zich hier enigszins gemakkelijk tot heel gemakkelijk te voelen. Dit klopt met de eerdere cijfers over het kleine aandeel respondenten dat het geen probleem vond om gegevens te verstrekken in ruil voor gratis online-diensten (14,9%).

Het hoge percentage respondenten dat 'neutraal' heeft geantwoord, kan er op wijzen dat zij niet goed weten wat zij er van moeten denken of niet goed kunnen inschatten wat de gevolgen zijn van het delen van persoonsgegevens in ruil voor gratis diensten. Het percentage respondenten dat zich er ongemakkelijk bij voelt is echter veel groter (37,7%) dan het percentage dat zich er gemakkelijk bij voelt (17,4%), wat doet vermoeden dat het ongemakkelijke gevoel overheerst – ook onder de neutraal stemmers.

*Figuur 10*
**DELEN VAN GEGEVENS VOOR BETERE ADVERTENTIEDIENSTEN**
SOMMIGE INTERNETBEDRIJVEN LEVEREN GRATIS DIENSTEN IN RUIL VOOR UW PERSOONSGEGEVENS, WELKE ZE VERVOLGENS WEER DOORVERKOPEN AAN DERDEN.




Als we dit correleren met de algemene houding tegenover privacy, dan blijkt dat respondenten die het normaal vinden om informatie te delen ook geen moeite hebben met het leveren van persoonsgegevens in ruil voor gratis diensten (.346).

### 4.3.5 TECHNOLOGIE

Om de veiligheid in Nederland te waarborgen, worden er verschillende technologieën ingezet. Daarbij kan gedacht worden aan camera's op straat of bodyscanners op een vliegveld. Deze technologieën verzamelen informatie over mensen, zoals beeldmateriaal met gezichten of gedrag of een scan van het lichaam. Met de informatie die verzameld wordt, kunnen kwaadwillende personen sneller geïdentificeerd of achterhaald worden. De verzamelde informatie is echter ook zeer privacygevoelig en daarmee van invloed op de privacybeleving.

**Privacygevoelige technologieën**

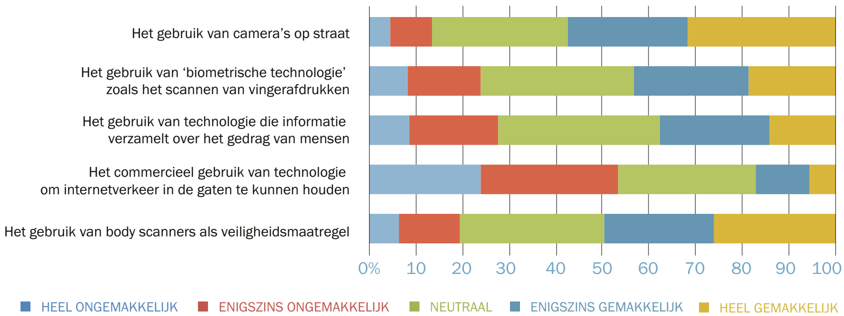
In Figuur 11 is te zien hoe gemakkelijk of ongemakkelijk men zich voelt bij het gebruik van deze technologieën. Het grootste aantal respondenten voelt zich enigszins ongemakkelijk of heel ongemakkelijk bij technieken die voor commerciële doeleinden het internetverkeer in de gaten te houden: 53,6% van de respondenten geeft dit aan. Een aanzienlijk kleiner aandeel voelt zich ongemakkelijk bij de aanwezigheid van camera's op straat: 13,5% voelt zich er enigszins of heel gemakkelijk bij. Ook bodyscanners worden door een relatief kleine groep negatief ervaren (19,4%). Toch ervaart nog steeds 1 tot 2 op de 10 respondenten ongemakkelijkheid bij deze technologieën.

Het valt op dat bij de beantwoording van deze vraag (offline) technologieën zoals camera's en bodyscanners, die duidelijk zichtbaar zijn in het straatbeeld en zich op steeds meer plekken manifesteren, meer geaccepteerd worden dan (online)technologieën die voor de gebruiker onzichtbaar zijn, zoals technologieën voor het monitoren van internetverkeer.

*Figuur 11*

**GEVOEL BIJ TECHNOLOGIEËN DIE PERSOONSGEGEVENS REGISTREREN**

HOE VOELT U ZICH BIJ DE VOLGENDE TECHNOLOGIEËN DIE IN NEDERLAND GEBRUIKT WORDEN?




Als we nader inzoomen op het effect van deze technologieën op de algemene privacybeleving, dan blijkt dat mensen die de bescherming van hun persoonsgegevens belangrijk vinden wat minder moeite hebben met camera's op straat (.195) en bodyscanners (.147), maar wel weer iets meer moeite hebben met het monitoren van internetverkeer voor commercieel gebruik (-.165). Daarentegen hebben de respondenten die het normaal vinden om gegevens op internet te delen minder moeite met dit monitoren (.225). Ook hebben zij significant minder moeite met het gebruik van de andere technologieën.

### 4.3.6 INVLOED EN CONTROLE

In de theorie stelden we dat de mate van invloed die mensen zelf kunnen uitoefenen op de diensten die zij gebruiken en de controle die zij hebben over het gebruik hun gegevens, van invloed is op de beleving van privacy. Wanneer iemand meer controle heeft, leidt dit tot een beter gevoel van bescherming van privacy.

**Behoefte aan controle**

Om een beeld te krijgen van de behoefte om controle uit te oefenen over het gebruik van persoonsgegevens, hebben we respondenten gevraagd hoe belangrijk zij bepaalde vormen van controle vinden. We hebben onderscheid gemaakt naar het belang van privacy in relatie tot het anoniem gebruik kunnen maken van internet (online privacy), het deelnemen aan een demonstratie zonder gemonitord te worden (fysieke privacy) en het hebben van controle over wie gegevens kunnen inzien (privacy van informatie). Dit onderscheid in privacyaspecten is gebaseerd op het Europese onderzoeksproject PRISMS waar TNO bij betrokken is.

In Figuur 12 is te zien dat vrijwel alle vormen van controle over privacy belangrijk worden gevonden door de respondenten uit dit onderzoek. We zien bevestigd wat we in de theorie al stelden: veruit het meeste belang wordt gehecht aan het controleren van inzage in persoonsgegevens: ruim 80% van de respondenten geeft aan dit belangrijk of heel belangrijk te vinden. Andere onderwerpen waar veel waarde aan wordt gehecht zijn het kunnen voeren van telefoongesprekken zonder dat overheden mee kunnen luisteren (76,6%), het weten wie informatie over de respondent heeft (72,5%) en het anoniem gebruik kunnen maken van internet (72,5%). Het privé kunnen houden van religieuze ideeën (38,3%) en het kunnen deelnemen aan een demonstratie zonder in de gaten te worden gehouden door de overheid (47,8%) worden relatief minder belangrijk gevonden. Opvallend is dat relatief veel mensen hier ‘neutraal’ antwoorden (respectievelijk 31,5% en 31,3%).

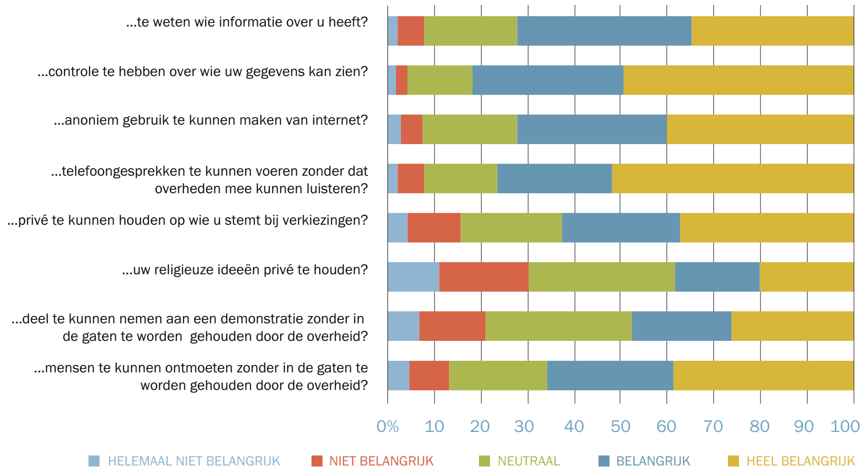
Overigens moet hier opgemerkt worden dat de percentages een licht vertekend beeld geven, omdat deze – onder invloed van de eerder genoemde aanslagen in Parijs op 7 januari 2015 (zie Hoofdstuk 2: Methode) – iets afwijken: respondenten die de vragenlijst hebben ingevuld ná de aanslagen blijken iets minder moeite te hebben met het afluisteren van hun telefoon, het niet kunnen deelnemen aan demonstraties en het ontmoeten van mensen zonder dat de overheid mee kijkt. Die percentages liggen normaliter dus iets hoger.

Opvallend is dat de privacyaspecten waar veel waarde aan wordt gehecht, samenhangen met online privacy en privacy van informatie (de eerste vier items). Het lijkt erop dat vooral in situaties die als privé gelden, dus binnenshuis of in een besloten kring, privacy voorop staat. In meer openbare situaties, dus buiten op straat of in een grotere groep, wordt minder belang aan privacy toegekend. Er lijkt dus een verband met de mate van beslotenheid en de privacyverwachting die daar bij hoort.

*Figuur 12*

**BEHOEFTE AAN CONTROLE OVER PRIVACY**

HOE BELANGRIJK VINDT U HET OM...




**Controle over persoonsgegevens**

Wanneer mensen het gevoel hebben goed te kunnen controleren wie er bij hun persoonlijke informatie kan en wat hiermee gebeurt, zijn zij wellicht minder bezorgd over hun privacy en het gebruik van hun persoonsgegevens. Daarom is aan de respondenten een aantal vragen gesteld over het gevoel van controle dat zij hebben over de toegang tot en het gebruik van hun gegevens.

Uit Figuur 13 komt een beeld naar voren van respondenten die over het algemeen of zeker weten waarvoor hun persoonsgegevens worden gebruikt (39,4%). Slechts 12,1% van alle respondenten zegt ook te weten wie er bij de gegevens kan. Dit percentage steek schril af bij de grote groep respondenten die niet of niet zeker weet wie er bij de gegevens kan: 50,8% dus meer dan de helft van de respondenten zegt hier onzeker over te zijn.

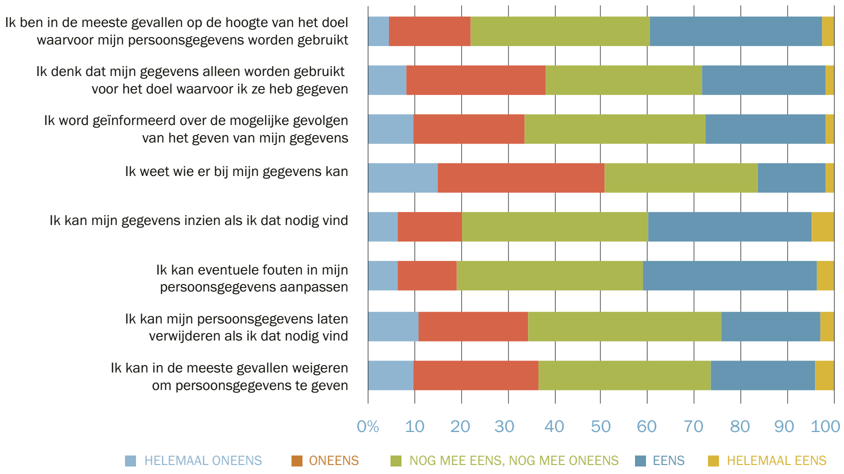
Met name als het gaat om het kunnen inzien en het aanpassen van persoonsgegevens, wordt vaak gekozen voor de antwoordmogelijkheid ‘noch mee eens, noch mee oneens’ (beiden 40,1%). Dit lijkt er op te wijzen dat de respondenten niet helemaal zeker weten of dit kan of niet. Ruim één derde van de respondenten (respectievelijk 35% en 37,1%) denkt dat het wel mogelijk is om te kunnen zien wie er bij de gegevens kunnen. Bij de mogelijkheid voor het verwijderen van persoonsgegevens antwoordt 41,2% ‘niet mee eens, noch mee oneens’, terwijl 34,4% denkt dat dit niet kan. Voor het weigeren van het delen van persoonsgegevens zien we hetzelfde gebeuren: 36,8% twijfelt of dit kan, terwijl 26,9% denkt dat dit niet kan.

De hoge percentages ‘niet mee eens, noch mee oneens’ kunnen er op duiden dat de respondenten onzeker zijn over het gebruik en beheer van persoonsgegevens. Ze lijken wel het gevoel te hebben dat ze hun gegevens kunnen aanpassen en in kunnen zien als ze dat nodig vinden, maar ze zijn er minder van overtuigd dat ze kunnen weigeren om hun persoonsgegevens te delen of dat ze hun gegevens kunnen laten verwijderen.

*Figuur 13*

**MATE VAN CONTROLE OVER PERSOONSGEGEVENS**

GEEF VOOR DE VOLGENDE UITSPRAKEN AAN IN HOEVERRE U HET HIER MEE EENS OF ONEENS BENT




We hebben onderzocht of er een verband bestaat tussen de mate van controle die mensen ervaren over hun gegevens en het al dan niet verstrekken van deze gegevens: zijn mensen die meer controle ervaren ook sneller geneigd om hun gegevens te verstrekken en vice versa? Hiervoor is in dit onderzoek geen signficant bewijs gevonden. Wel blijkt er een signficant (zwak) verband te bestaan tussen het weten wie er bij gegevens kan en het belang dat men hecht aan de bescherming van persoonsgegevens: de respondenten die bescherming van persoonsgegevens belangrijk vinden en vinden dat er in de maatschappij over gesproken moet worden, geven ook aan minder goed te weten wie er bij de gegevens kan (respectievelijk -.116 en -.155). De mensen die het normaal vinden om gegevens te delen geven iets vaker aan ook te weten wie er bij de informatie kan (.186).

**Privacybeschermende technieken**

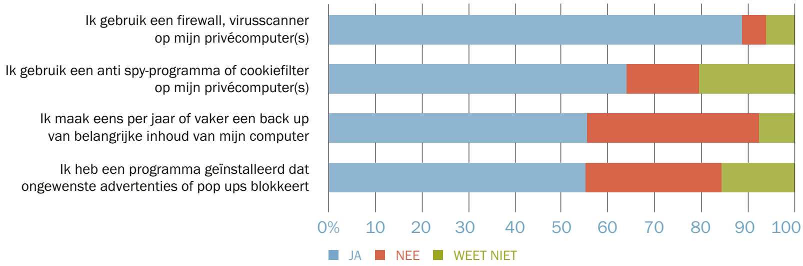
Die controle over het gebruik van gegevens kan op verschillende manieren worden uitgeoefend: door het installeren van beschermende technieken of door het vertonen van beschermend gedrag. Bij technieken moeten er gedacht worden aan het installeren van beschermende software. Bij gedrag gaat het meer om handelingen zoals het wisselen van wachtwoorden en het doen van navraag bij instellingen die persoonsgegevens beheren.

De respondenten is gevraagd welke technieken zij gebruiken om hun gegevens te beschermen. In Figuur 14 is te zien dat het overgrote deel van de respondenten zegt een firewall of virusscanner te gebruiken (88,5%). Deze maatregel wordt het meest getroffen. Verder gebruikt een ruime meerderheid (63,8%) een anti-spyprogramma of cookiefilters. De anti-spyprogramma's, cookiefilters en programma's die ongewenste advertenties of pop-ups blokkeren, blijken voor enkele respondenten relatief onbekend te zijn, aangezien respectievelijk 20,6% en 15,9% hier 'weet niet' antwoordt. Het controleren van URL's, het maken van back-ups of het installeren van een pop-up blocker wordt door iets meer dan de helft van de respondenten gedaan.

*Figuur 14*

**GEBRUIK VAN TECHNIEKEN OM PERSOONSGEGEVENS TE BESCHERMEN**

WELKE VAN DE ONDERSTAANDE HANDELINGEN ZIJN OP U VAN TOEPASSING




De verwachting was dat mensen die meer gebruik maken van technische tools, ook anders zouden omgaan met het verstrekken van hun persoonsgegevens. Er blijkt inderdaad een zwak significant verband te zijn bij het controleren van het webadres (-.107) en het gebruik van pop-up blockers (-.115). De mensen die dit doen of deze techniek hebben geïnstalleerd, zijn dus iets voorzichtiger met het delen van hun gegevens.

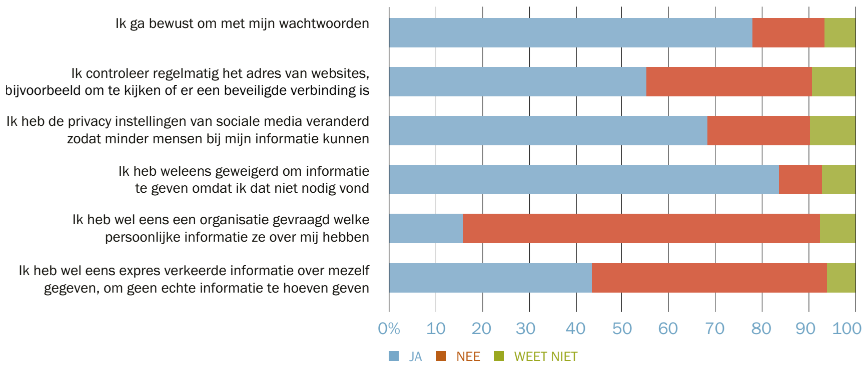
**Privacybeschermend gedrag**

Naast terughoudendheid bij het verstrekken van gegevens, is ook ander privacybeschermend gedrag mogelijk. We hebben de respondenten gevraagd of zij dit gedrag wel eens vertonen. Zie hiervoor Figuur 15. Van de respondenten zegt 77,6% bewust om te gaan met zijn of haar wachtwoorden, 55,7% controleert het adres van de websites. Ook wordt het profiel op sociale media afgeschermd (68,4%) of er wordt wel eens geweigerd informatie te geven (83,7%), maar slechts een klein deel heeft ook echt navraag gedaan over de informatie die een bepaalde organisatie bezit (16%).

*Figuur 15*

**GEDRAG OM PERSOONSGEGEVENS TE BESCHERMEN**

WELKE VAN DE ONDERSTAANDE HANDELINGEN ZIJN OP U VAN TOEPASSING?

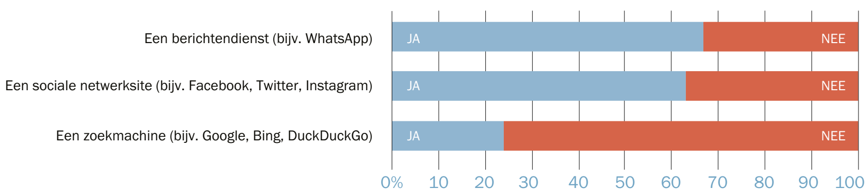


Dit gedrag staat natuurlijk niet op zichzelf, maar komt mogelijk ook voort uit de algemene houding die mensen hebben ten aanzien van privacy en de bescherming van persoonsgegevens.
We hebben onderzocht of dit verband ook significant is: respondenten die het belangrijk vinden dat hun gegevens beschermd worden vinden, zijn inderdaad iets actiever geweest in het aanpassen van hun instelling op sociale media (.135) en hebben ook wel eens info geweigerd (.150).
Opvallend is dat juist deze respondenten minder geneigd zijn om navraag te doen bij organisaties over de persoonsgegevens waarover zij beschikken (-.156). Er blijkt ook een zwak negatief verband te bestaan voor de respondenten die het geen probleem vinden om hun gegevens te ruilen voor gratis diensten: zij zijn iets minder geneigd om het te weigeren als er om hun gegevens wordt gevraagd (-.115).

**Peer pressure**
Hoewel de respondenten hebben aangegeven sociale media minder te vertrouwen en onzeker te zijn over het gebruik van hun persoonsgegevens door derden, maken veel mensen toch gebruik van dergelijke diensten. Dit is onder andere het gevolg van *peer pressure*: omdat familie, vrienden en collega's gebruik maken van de diensten, voelen mensen zich vaak gedwongen om dit ook te doen.

Uit de survey blijkt dat 41,3% van de respondenten wel eens het gevoel heeft dat hij of zij gebruik maakt van een digitale dienst omdat bijna iedereen in zijn of haar omgeving dit doet, terwijl 48,5% dit niet zo ervaart. De overige 10,2% weet het niet of heeft geen mening. Wanneer we verder inzoomen op de diensten waarvan men het gevoel heeft deze te moeten gebruiken vanwege druk uit de omgeving, (zie Figuur 16), dan blijkt het voornamelijk te gaan om diensten als WhatsApp en sociale netwerksites zoals Facebook, Twitter en Instagram. En dit zijn juist de diensten waarvan men eerder aangaf deze weinig te vertrouwen bij de bescherming en doelmatig gebruik van persoonsgegevens (74,8% van de respondenten had hier weinig tot zeer weinig vertrouwen in).
Ondanks het weinige vertrouwen, toch gebruik maken van deze diensten hangt naast peer pressure mogelijk ook samen met *the fear of missing out*: bang zijn om belangrijke gebeurtenissen en ontwikkelingen te missen wanneer zij niet deelnemen aan dezelfde online platformen als vrienden en familie.

*Figuur 16*
**TYPE DIENSTEN WAARAAN DOOR PEER PRESSURE WORDT DEELGENOMEN**
BIJ WELK TYPE DIENST VOELDE U DRUK VAN UW OMGEVING OM OOK DEEL TE NEMEN?



### 4.3.7 AWARENESS

De laatste factor die we hebben gemeten is ‘awareness’: de kennis die de respondenten hebben over het maatschappelijk veld dat zich bezighoudt met privacy en de bescherming van persoonsgegevens. Ook hebben we hier gekeken naar de mate waarin de respondenten zich bezighouden met het de bescherming van hun persoonsgegevens en de risico’s die ontstaan door het gebruik van internet.

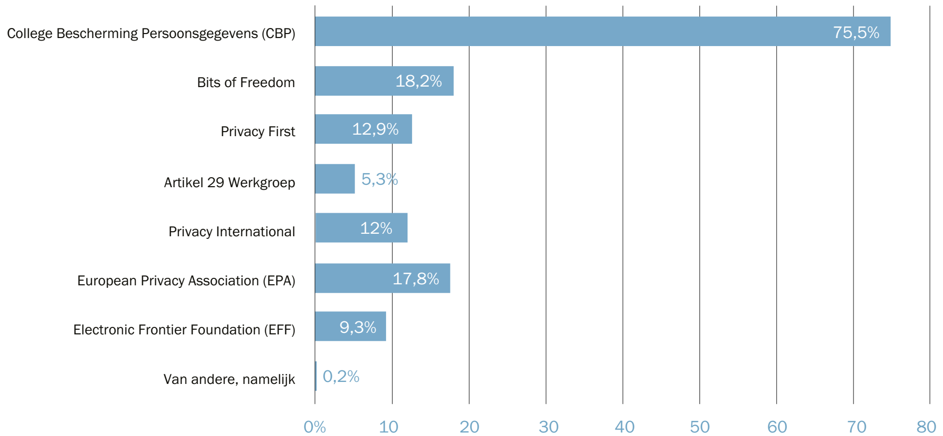
**Kennis van maatschappelijk speelveld**

We hebben de respondenten gevraagd aan te geven welke van de genoemde instanties die zich bezighouden met privacy en bescherming van persoonsgegevens zij kennen (zie Figuur 17).
De verwachting was dat mensen die bescherming van persoonsgegevens belangrijk vinden, ook beter bekend zijn met de instanties die deze bescherming waarborgen. Een ruime meerderheid van de respondenten (75,5%) geeft aan gehoord te hebben van het College Bescherming Persoonsgegevens (CBP). De overige organisaties zijn minder bekend bij de respondenten: 18,2% kent Bits of Freedom en 17,8% van de respondenten kent de European Privacy Associatie (EPA).

De bekendheid van het grote publiek met de zeven meest vooraanstaande instanties die privacy en bescherming van persoonsgegevens bespreekbaar maken en waarborgen, blijkt helaas beperkt te zijn. Alleen de belangrijkste toezichthouder, het CBP, is bij het grote publiek bekend.

*Figuur 17*

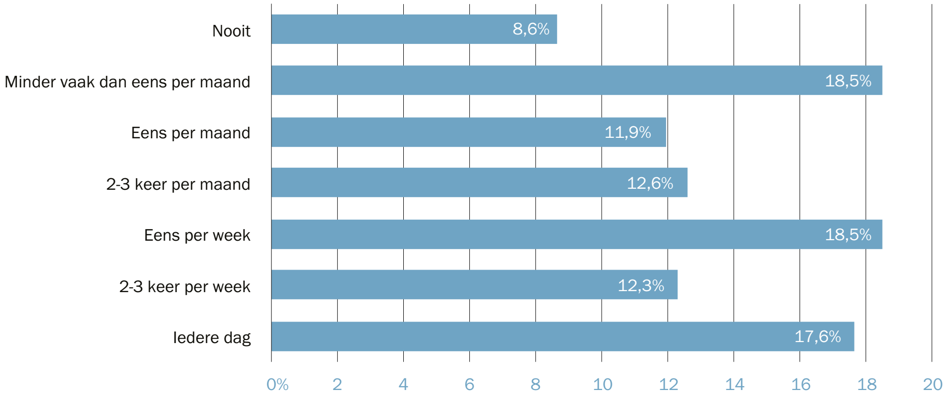
**BEKENDHEID MET INSTANTIES DIE ZICH BEZIGHOUDEN MET PRIVACY EN BESCHERMING VAN PERSOONSGEGEVENS** HEEFT U WEL EENS GEHOORD VAN DEZE INSTANTIES (IN NEDERLAND EN DAARBUITEN) DIE ZICH BEZIG HOUDEN MET PRIVACY EN BESCHERMING VAN PERSOONSGEGEVENS?



**Aandacht voor de bescherming van persoonsgegevens**
Aan het begin van de analyse hebben we onderzocht welk belang mensen hechten aan de bescherming van persoonsgegevens (zie Figuur 1). Daar gaf 71,2% van de respondenten aan het belangrijk te vinden dat de bescherming van persoonsgegevens een onderwerp is waar in de maatschappij aandacht voor is. In vervolg hier op hebben we respondenten gevraagd hoe vaak ze zelf nadenken over de risico's voor hun persoonsgegevens door het gebruik van internet.
Ook hebben we de respondenten gevraagd in hoeverre zij zelf aandacht vragen voor dit onderwerp.

In Figuur 18 is te zien dat 17,6% van de respondenten zegt iedere dag na te denken over wat er kan gebeuren met zijn of haar persoonsgegevens bij het gebruik van internet. Ongeveer evenveel respondenten zeggen eens per week (18,5%) of minder vaak dan eens per maand (18,5%) na te denken over de gevolgen van het gebruik van internet voor persoonsgegevens. Slechts een klein deel van de respondenten (8,6%) zegt nooit over de risico's voor persoonsgegevens bij gebruik van internet na te denken. Het merendeel van de Nederlanders denkt dus wel met enige regelmaat na over de risico's van persoonsgegevens bij internetgebruik.

*Figuur 18*
**NADENKEN OVER WAT ER MET PERSOONSGEGEVENS KAN GEBEUREN**
HOE VAAK DENKT U IN HET ALGEMEEN NA OVER WAT ER BIJ HET GEBRUIK VAN INTERNET KAN GEBEUREN MET UW PERSOONSGEGEVENS?

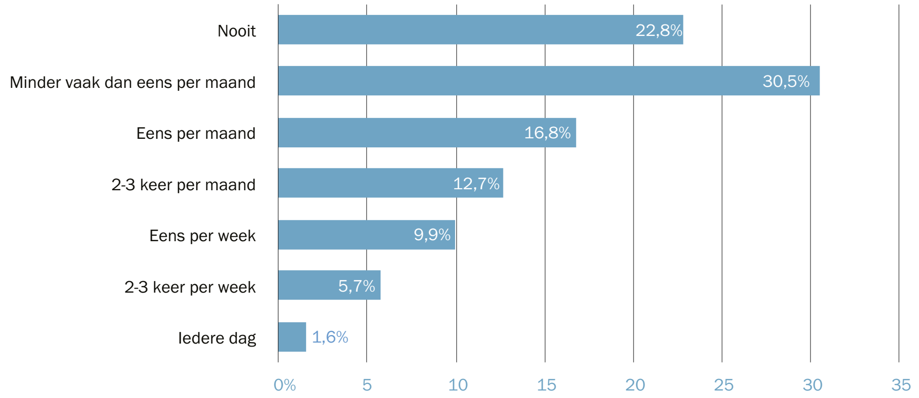



Om te meten in hoeverre de respondenten zelf ook aandacht vragen voor het onderwerp, is hen gevraagd naar het aantal keren dat ze met andere mensen *praten* over het gebruik van eigen of andermans persoonsgegevens door overheden en bedrijven (zie Figuur 19). Het grootste deel van de respondenten zegt hier wel over te praten (77,2%), de overige 22,8% zegt hier nooit met anderen over te spreken. De grootste groep spreekt er minder dan eens per maand over (30,5%), terwijl 17,2% er eens per week of vaker met anderen over spreekt.

*Figuur 19*

**MET ANDERE MENSEN PRATEN OVER HET GEBRUIK VAN PERSOONSGEGEVENS**

HOE VAAK PRAAT U MET ANDERE MENSEN OVER HET GEBRUIK VAN UW OF ANDERMANS PERSOONSGEGEVENS DOOR OVERHEDEN OF BEDRIJVEN?

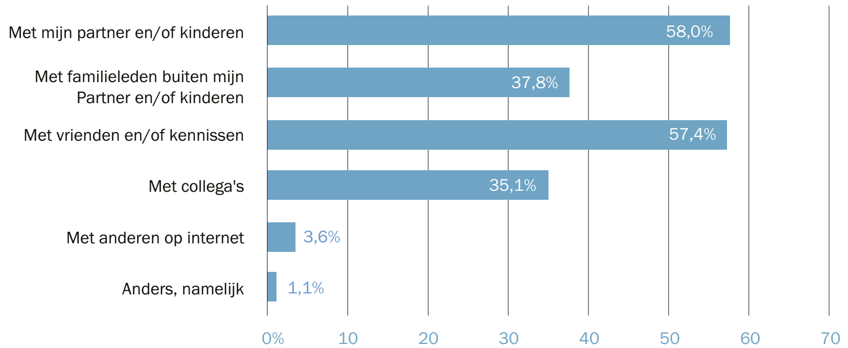



Aan de mensen die wel eens met anderen praten over het gebruik van persoonsgegevens door overheden of bedrijven, is de vervolgvraag gesteld met wie ze hier dan over spreken (zie Figuur 20). De meeste mensen die hier wel eens over praten, doen dit voornamelijk met hun partner en/of kinderen (58%) en hun vrienden en/of kennissen (57,4%). Er wordt maar weinig met anderen op internet over dit thema gesproken (3,6%).

*Figuur 20*

**MET WIE PRATEN OVER GEBRUIK VAN PERSOONSGEGEVENS**

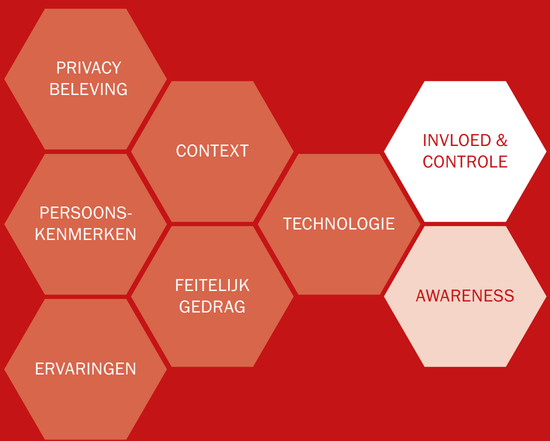
INDIEN U MET ANDERE MENSEN PRAAT OVER HET GEBRUIK VAN UW OF ANDERMANS PERSOONSGEGEVENS DOOR OVERHEDEN OF BEDRIJVEN, MET WIE PRAAT U HIER DAN OVER?



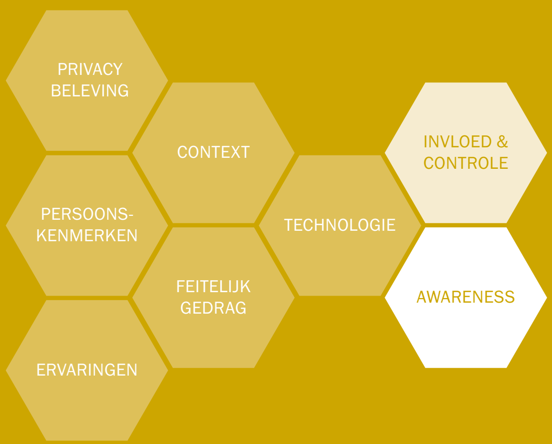
Het merendeel van de respondenten vraagt dus bij voornamelijk familie en vrienden aandacht voor de bescherming van persoonsgegevens, maar doet dit slechts af en toe. Een kleine groep (7,3%) spreekt hier echter wel (vrijwel) dagelijks over.

Als we het nadenken en spreken over de bescherming van persoonsgegevens afzetten tegen het algemeen belang dat aan privacy wordt gehecht, dan zien we eenzelfde trend als in de rest van de analyse: de respondenten die de bescherming van persoonsgegevens belangrijk vinden en ook vinden dat er over gesproken moet worden in de maatschappij, die zijn ook iets meer geneigd om er over na te denken (respectievelijk .153 en .135). De respondenten die het normaal vinden om gegevens te delen en dit ook doen in ruil voor gratis diensten, denken er ook iets minder over na (respectievelijk -.110 en .141). De algemene houding tegenover privacy blijkt geen significante relatie te hebben met de frequentie waarmee de respondenten met de omgeving over de bescherming van persoonsgegevens spreken.

# HOE BELANGRIJK VINDT **U HET OM CONTROLE TE HEBBEN OVER WIE UW GEGEVENS KAN INZIEN?**



# HOE VAAK PRAAT **U MET ANDEREN OVER UW ONLINE PRIVACY?**



# 5 CONCLUSIE

UIT HET ONDERZOEK BLIJKT DAT DE NEDERLANDSE BEVOLKING RELATIEF VEEL BELANG HECHT AAN PRIVACY EN DE BESCHERMING VAN PERSOONSGEGEVENS. IN DIT LAATSTE HOOFDSTUK BESPREKEN WE PER FACTOR DE BELANGRIJKSTE UITKOMSTEN VAN HET ONDERZOEK EN PLAATSEN WE HET IN HET PERSPECTIEF VAN DE ALGEHELE PRIVACYBELEVING.

Men hecht belang aan privacy en de bescherming van persoonsgegevens. Er worden ook concrete acties ondernomen om persoonsgegevens te beschermen, zoals het installeren van beschermende software of het aanpassen van profielinstellingen. Tegelijkertijd is er veel onduidelijkheid over hoe mensen meer controle kunnen uitoefenen over hun persoonsgegevens en het gebruik daarvan door anderen, met name door commerciële partijen. Men heeft weinig vertrouwen in een goede omgang met hun persoonsgegevens door commerciële partijen, zoals webwinkels, sociale netwerksites, en ook goede doelenorganisaties. Tegelijkertijd nemen mensen wel deel aan sociale netwerksites, onder andere omdat de omgeving daar om vraagt. Ook is er een groep internetgebruikers die weinig moeite heeft met het delen van persoonsgegevens in ruil voor een gratis dienst. De privacy paradox kent enige nuance.

## 5.1 DE ZEVEN FACTOREN IN RELATIE TOT DE PRIVACYBELEVING

**Persoonskenmerken**

Er blijken geen significante verschillen te bestaan tussen mannen en vrouwen. Ook het opleidingsniveau en de hoeveelheid tijd die men op het internet doorbrengt blijken geen significante relatie te hebben met het denken over privacy. Leeftijd daarentegen hangt wel samen met de bereidheid om gegevens te delen: jong volwassenen (tussen de 18 en 34 jaar) blijken de bescherming van persoonsgegevens minder belangrijk te vinden. Dit komt onder andere doordat zij het delen van informatie een vanzelfsprekendheid vinden in de huidige maatschappij. Over de gehele breedte van het onderzoek blijken deze jong volwassenen minder moeite te hebben met het delen van gegevens en treden zij ook minder beschermend op.

**Ervaringen**

Van de respondenten heeft 17,4% aangegeven weleens slachtoffer te zijn geweest van verlies of diefstal van hun persoonsgegevens. In meer dan de helft van de gevallen is dat ook het afgelopen jaar gebeurd. De meeste incidenten betreffen het zonder toestemming doorgeven van de gegevens aan een andere organisatie dan de organisatie die de gegevens van de persoon had verkregen. Daarnaast is 1 op de 10 mensen (10,3%) weleens slachtoffer geweest van identiteitsfraude.
De meest voorkomende vorm van identiteitsfraude is online identiteitsfraude, gevolgd door financiële identiteitsfraude. De veronderstelling was dat mensen die te maken hebben gehad met verlies, diefstal of fraude ook voorzichtiger zouden zijn bij het delen van hun persoonsgegevens en

meer beschermende maatregelen zouden treffen. Er blijkt alleen een zwak maar significant verband te bestaan tussen de wens om een debat over de bescherming van persoonsgegevens en het bewustzijn slachtoffer te zijn van verlies of diefstal van gegevens. Mogelijk dat dit verband sterker is, als het percentage mensen dat bewust is slachtoffer te zijn van verlies of diefstal van gegevens, hoger ligt. De cijfers hierboven betreffen namelijk de gevallen waarin de respondenten op de hoogte zijn van de fraude of het verlies van hun gegevens. In werkelijkheid is het aantal slachtoffers mogelijk hoger.

Tot slot hebben we de respondenten gevraagd naar het vertrouwen in de overheid en de wet- en regelgeving om persoonsgegevens te beschermen. Bij deze vragen bleken respondenten vaak voor ‘noch mee eens, noch mee oneens’ te kiezen. Daardoor ontstaat het beeld dat mensen onbekend zijn met de aandacht die de aandacht die de overheid besteedt aan het beschermen van persoonsgegevens en aan de effectiviteit van de wetgeving en de getroffen maatregelen. Ook is voor de meeste mensen onduidelijk of de wetgeving voldoende bescherming biedt.

**Feitelijk gedrag**
Op het internet wordt voornamelijk gebruik gemaakt van zoekmachines, het bekijken van foto’s en video’s van anderen op sociale media en het versturen van berichten via diensten als WhatsApp. Hoewel mensen graag foto’s van anderen bekijken, zeggen ze zelf zelden foto’s op sociale media te plaatsen.

Ook is gebleken dat het gebruik maken van diensten vaak doorslaggevend is in de afweging of iemand wel of geen persoonsgegevens deelt. Bij het gebruik van diensten zien we ook weer de groep jongvolwassenen terug die het normaal vinden om informatie te delen: zij zijn meer dan anderen geneigd hun gegevens te delen. Dit doen ze overigens voor alle typen diensten en zelfs iets meer voor webwinkels en zoekmachines. Slechts 14% van de respondenten geeft aan helemaal geen gegevens te delen als daar om wordt gevraagd, met als gevolg dat zij bepaalde diensten niet kunnen gebruiken.

Er is dan ook sprake van een privacy paradox: het belang van privacy wordt door het overgrote deel van de mensen benadrukt, maar toch worden gegevens vaak verstrekt als daar om wordt gevraagd. Een grote groep (bijna 30%) verstrekt de gegevens alleen als de dienst anders niet gebruikt kan worden. Toegang tot de dienst gaat in die gevallen dus voor privacy en daarmee verliest de internetgebruiker controle over die gegevens. Wel is er enige nuance noodzakelijk. Uit de survey blijkt dat een groot deel van de respondenten (bijna 40%) van de respondenten alleen gegevens geeft als duidelijk is waarvoor dat nodig is. Er wordt dus in veel gevallen wel degelijk een sterke afweging gemaakt, waarbij niet alleen de toegang tot de dienst meetelt, maar ook het mogelijke gebruik van de gegevens en de noodzakelijkheid van het verzamelen van de gegevens in relatie tot de gewenste dienst.

Net als in Canada en Australië, leest bijna de helft van de Nederlanders de algemene voorwaarden. Dat percentage is relatief hoog, als we in ogenschouw nemen dat de algemene voorwaarden vaak ook onduidelijk en lang worden gevonden.

**Context**
De bescherming die mensen verlangen voor hun persoonsgegevens, hangt in grote mate af van de context waarin gegevens gevraagd worden. En van het vertrouwen dat mensen hebben in een organisatie.

Overheidsorganisaties zoals de politie en de belastingdienst, maar ook de gezondheidszorg, werkgevers, verzekeraars en banken worden meer vertrouwd in het gebruik en de bescherming van persoonsgegevens dan commerciële organisaties zoals webwinkels, goede doelenorganisaties en marktonderzoeksbureaus. Ook het vertrouwen in sociale media blijkt significant lager te liggen.

**Technologie**
Het type technologie dat gebruikt wordt heeft ook invloed op de privacybeleving van de respondenten. Zo worden camera's en bodyscannersslechts door een beperkte groep als negatief ervaren, terwijl technologieën die voor commerciële doeleinden het internetgedrag monitoren door meer dan de helft van de respondenten als negatief ervaren worden. Het valt daarbij op dat de technologieën die in de fysieke ruime zichtbaar zijn en beelden maken, meer geaccepteerd worden dan technologieën die online worden gebruikt en gegevens verzamelen. Dit kan te maken hebben met een relatief van gevoel van controle, wanneer men een technologie kan zien en dus weet wanneer er gegevens verwerkt worden. Het echte verschil lijkt echter afhankelijk van de context. De zichtbare technologieën uit de vragenlijst zijn bestemd voor beveiliging en openbare orde. Dat wordt over het algemeen geaccepteerd. Wanneer er echter technologie wordt ingezet met een commercieel doel, dan is de acceptatiegraad beduidend lager. Deze verklaring past ook beter bij de houding die gebruikers hebben ten opzichte van bijvoorbeeld sociale media platformen en webwinkels.

**Invloed en controle**
Vrijwel alle vormen van controle over privacy worden belangrijk gevonden, waarbij veruit het meeste belang wordt gehecht aan het controleren van toegang tot persoonsgegevens, het kunnen voeren van telefoongesprekken zonder dat overheden meeluisteren, het weten wie over persoonsgegevens beschikt en het anoniem kunnen gebruiken van internet. Hierbij dient overigens de kanttekening geplaatst te worden dat de acceptatie van het afluisteren van telefoongesprekken, het niet kunnen deelnemen aan demonstraties en het ontmoeten van mensen zonder dat de overheid mee kijkt iets vertekend zijn. Door de aanslagen in Parijs in januari dit jaar hebben de respondenten aangegeven met deze vormen van monitoring iets minder moeite te hebben, mogelijk vanuit de veronderstelling dat de veiligheid beter gegarandeerd kan worden. Het belang dat doorgaans aan privacy in deze verbanden wordt gehecht ligt mogelijk dus nog iets hoger.

Het valt op dat de vormen van privacy waaraan veel belang wordt gehecht, samenhangen met online privacy en privacy van informatie. Het zijn vooral situaties die in besloten kring of binnenshuis plaatsvinden die privacygevoelig worden gevonden. In meer openbare situaties wordt minder belang gehecht aan privacy. Er lijkt dus een verband te bestaan tussen de mate van beslotenheid en de privacy verwachting die daarbij hoort.

Hoewel veel respondenten aangeven verschillende vormen van controle belangrijk te vinden, bestaat er veel onduidelijkheid over de mogelijkheden om controle uit te oefenen op verwerkte persoonsgegevens. Vaak hebben mensen wel een idee welke gegevens worden verwerkt, maar weten ze niet of ze die gegevens ook kunnen inzien om ze te controleren. Ook is voor veel mensen onbekend wié er bij hun gegevens kan (slechts 12,1% van de respondenten zegt dit te weten).

Ook weten ze niet zeker of ze de gegevens kunnen inzien en aanpassen of (laten) verwijderen. Mensen hebben dus niet de overtuiging dat ze een zekere invloed en controle kunnen uitoefenen over hoe hun gegevens gebruikt worden en door wie. Dat gebrek aan controle en overzicht heeft een negatief effect op de privacybeleving.

Uit nadere analyse blijkt ook dat mensen die het belangrijk vinden dat hun persoonsgegevens beschermd worden en dat er een maatschappelijk debat over wordt gevoerd, ook iets onzekerder zijn over wie er bij de gegevens kan. Daarentegen geven de mensen die hun gegevens wel willen delen aan dat zij wel weten wie er bij hun gegevens kunnen komen.

Op de punten waar wel invloed of controle uitgeoefend kan worden, gebeurt dit ook. Het overgrote deel van de mensen gebruikt een firewall of virusscanner (88,5%) en ruim 77% gaat bewust om met wachtwoorden. Anti-spyprogramma's en cookiefilters worden door een ruime meerderheid gebruikt. Er worden dus wel degelijk technische maatregelen genomen om gegevens te beschermen en ook specifiek gericht op het voorkomen van monitoring van internetgedrag. De mensen die dit soort programma's hebben geïnstalleerd, blijken ook daadwerkelijk iets voorzichtiger in het delen van hun gegevens. Zij nemen meer technische maatregelen ter bescherming van gegevens en zijn daarnaast selectiever in het beschikbaar stellen van gegevens wanneer daar om gevraagd wordt. Tegelijkertijd blijkt dat de tools die monitoring tegengaan (anti-spyprogramma's, cookiefilters, pop-up blockers) ook nog relatief onbekend zijn, omdat ongeveer een vijfde van de respondenten niet weet of ze die gebruiken. Uiteindelijk blijkt controle vooral plaats te vinden in het niet verschaffen van gegevens of deze afschermen, bijvoorbeeld op sociale media. Actief navragen of inzage vragen is slechts door 15% ooit gedaan. Dit zijn opvallend genoeg juist niet de mensen die actief hun gegevens beschermen door het installeren van programma's en technieken: zij blijken iets minder actief navraag te doen bij instellingen die persoonsgegevens verwerken. De mogelijkheid tot controle leidt dus tot meer vertrouwen.

Hier blijkt de privacyparadox weer zichtbaar te worden: hoewel mensen belang hechten aan privacy en de bescherming van persoonsgegevens én ook beschermende software installeren, is men toch bereid om gegevens te delen als dit voor het gebruik van een dienst noodzakelijk is. Dit is onder andere het gevolg van de eerder genoemde 'peer pressure'. Meer dan 40% geeft aan weleens het gevoel te hebben dat ze wel aan een dienst deel moeten deelnemen, omdat iedereen in hun omgeving dat doet. Dit blijkt vooral het geval bij diensten als WhatsApp en sociale netwerksites, zoals Twitter en Facebook – juist de diensten waarvan men aangaf er weinig vertrouwen in te hebben. De druk kan dan puur uit de deelname voortkomen, dus om er bij te horen. Daarnaast speelt vaak de 'fear of missing out', waarbij men bang is nieuws of uitnodigingen te missen omdat die alleen via deze platformen worden gedeeld.

**Awareness**
De laatste factor die we gemeten hebben is de kennis van het maatschappelijk veld dat zich bezighoudt met privacy en de bescherming van persoonsgegevens. Van de genoemde instanties, blijkt het merendeel van de respondenten alleen het College Bescherming Persoonsgegevens te kennen. De overige organisaties blijken relatief onbekend te zijn bij het grote publiek. Mogelijk heeft dit ermee te maken dat het om specifieke organisaties gaat met een gericht boodschap en doel. Vaak zijn dergelijke organisaties alleen bekend bij mensen die gericht of actief met het onderwerp bezig zijn.

Het overgrote deel van de respondenten (71,2%) heeft aangegeven het belangrijk te vinden dat er over de bescherming van privacy en persoonsgegevens gesproken wordt. Van de respondenten denkt bijna 50% dagelijks of meerdere keren per week na over de risico's van internetgebruik voor persoonsgegevens. In verhouding tot de mensen die er over nadenken, spreekt echter een beperkte groep er met dezelfde regelmaat over: 17,2% van de respondenten spreekt er ook eens per week of vaker over. Er wordt dus veel over de risico's nagedacht, maar slechts in beperkte mate ook daadwerkelijk over gesproken.

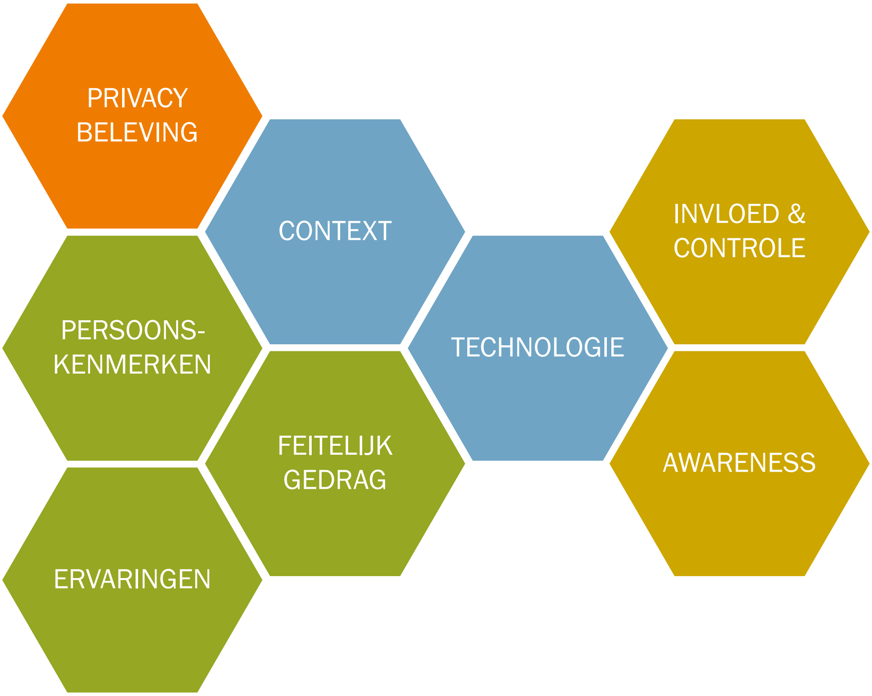
## 5.2 PRIVACYBELEVING IN BESCHOUWING

In het algemeen is er dus bewustzijn of awareness van privacy en wordt er belang gehecht aan de bescherming van persoonsgegevens, maar van actief gedrag is nog weinig sprake. Hoewel men privacybeschermende maatregelen treft, is men toch bereid om gegevens te delen als dit voor de toegang tot een dienst nodig is. Ook weet men niet goed wie er over de gegevens kan beschikken en of men zelf ook actief controle kan uitoefenen. Daarnaast bestaat er onbekendheid met het handelen van overheden.

Tenslotte kan gesteld worden dat consumenten vaak niet exact weten wat ze kunnen doen om hun gegevens te beschermen. Deels ligt dat aan het gebrek aan overzicht van wie er toegang hebben tot gegevens en wat er met die gegevens gebeurt. Consumenten kunnen het dus ook niet altijd weten. Bovendien blijkt dat er in de praktijk nog regelmatig persoonsgegevens onrechtmatig door derden worden doorgegeven aan andere partijen. Dat betekent dat consumenten niet altijd zelf de controle over hun gegevens kunnen hebben. Daarmee is vertrouwen in organisaties die gegevens verwerken een belangrijke factor voor de privacybeleving. Een andere oorzaak die leidt tot een verminderd gevoel van controle is peer pressure, waarbij de omgeving druk uitoefent om – ondanks bezwaren - toch gegevens te delen via bepaalde diensten.

Tegelijkertijd zien we dat consumenten vaak proberen controle te houden wanneer dat kan. Enerzijds gebeurt dat technisch, door beschermende software te installeren, anderzijds door zorgvuldig te zijn in het delen van gegevens. Opvallend is dat mensen die veel maatregelen hebben getroffen om gegevens te beschermen, zoals beschermende software installeren, veel minder vaak navraag doen naar het verwerken van hun gegevens.

De mogelijkheid tot controle en het gevoel van controle leiden dus tot meer vertrouwen in een zorgvuldige verwerking. Het onderwerp privacy wordt in het algemeen wel van belang gevonden en er wordt dan ook regelmatig over gesproken. Een goede privacybeleving blijkt van meerdere factoren en partijen afhankelijk te zijn. Mogelijkheden tot controle leiden tot meer vertrouwen, maar soms ontbreken die mogelijkheden ook.


PRIVACY BELEVING
CONTEXT
PERSOONS-KENMERKEN
TECHNOLOGIE
INVLOED & CONTROLE
FEITELIJK GEDRAG
AWARENESS
ERVARINGEN

## PERSOONLIJKE FACTOREN

### PERSOONS-KENMERKEN

- Leeftijd
- Geslacht
- Opleidingsniveau
- Intensiteit van internetgebruik

### ERVARINGEN

- Ervaringen verlies of diefstal van gegevens
- Ervaringen identiteitsfraude
- Optreden van overheden

### FEITELIJK GEDRAG

- Activiteiten online
- Bereidheid informatie te geven
- Lezen algemene voorwaarden en reglementen

## CONTEXTUELE FACTOREN

### CONTEXT

- Typen organisaties
- Doel verzamelen gegevens

### TECHNOLOGIE

- Type technologie voor verwerking gegevens

## RANDVOORWAARDEN SCHEPPENDE FACTOREN

### INVLOED & CONTROLE

- Behoefte aan controle
- Daadwerkelijke controle
- Privacybeschermende technieken
- Privacybeschermend gedrag
- Peer pressure/ fear of missing out

### AWARENESS

- Kennis van maatschap-pelijk speelveld
- Nadenken over risico's
- Praten over risico's

## TNO.NL

TNO VERBINDT MENSEN EN KENNIS OM INNOVATIES TE CREËREN DIE DE CONCURRENTIEKRACHT VAN BEDRIJVEN EN HET WELZIJN VAN DE SAMENLEVING DUURZAAM VERSTERKEN

Ook op het gebied van privacy en identiteit. TNO adviseert overheden en het bedrijfsleven bij de ontwikkeling van een integrale aanpak voor privacybeleid.

TNO innovation for life

